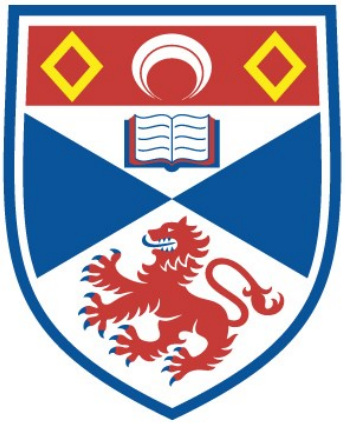
CENTRALISERS AND NORMALISERS IN SYMMETRIC AND ALTERNATING GROUPS

Huseyin Bilgiç

A Thesis Submitted for the Degree of PhD
at the
University of St Andrews



1998

CENTRALISERS AND NORMALISERS IN SYMMETRIC AND ALTERNATING GROUPS

Hüseyin Bilgiç [1]

Ph.D. Thesis
University of St Andrews
November 5, 1997

[1]Sponsored by Kahramanmaraş Sütçü İmam University, TURKIYE

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

To my parents,

my wife Özgül

and
my daughter Zeynep.

Contents

Declaration

I, Hüseyin Bilgiç, hereby certify that this thesis has been written by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree.

Date 05/11/1997. **Signature of candidate** .....

I was admitted as a research student in October, 1993 and as a candidate for the degree of Doctor of Philosophy in October, 1994; the higher study for which this is a record was carried out in the University of St Andrews between 1993 and 1997.

Date 05/11/1997. **Signature of candidate** .....

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Doctor of Philosophy in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree.

Date 05/11/1997. **Signature of supervisor** .....

In submission of this thesis to the University of St Andrews I understand that I am giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. I also understand that the title and abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or researh worker.

Date 05/11/1997. **Signature of candidate** .....

Acknowledgements

I would like to express my gratitude to my supervisor Dr J.J. O'Connor, who introduced me to the subject of computational group theory, for his ideas, guidance and invaluable advice.

Apart from my supervisor, I am very grateful to the members of School of Mathematical and Computational Sciences at the University of St Andrews for their support. My thanks is also to Dr Werner Nickel for the useful discussions about the GAP package and also to Ben Soares for the invaluable suggestions about LaTeX.

I would also like to thank Kahramanmaraş Sütçü İmam University for financial support.

Finally, I would like to thank my family whose patience, support and encouragement have made this work possible.

Abstract

In this thesis, we analyse the structure of the centraliser of an element and of the normaliser of a cyclic subgroup in both S_n and A_n.

We show that the centraliser in S_n of a permutation can be written as a direct product of centralisers of regular permutations and that the centraliser of a regular permutation is a wreath product. In certain cases we prove that this wreath product splits as a direct product and we analyse the centre of the subgroup.

We calculate the centraliser of a general permutation in A_n and show how this is related to the centralisers of regular permutations.

We investigate the normaliser of the cyclic subgroup generated by an element of S_n and show how this is related to the centraliser of the permutation. We calculate the centre of the normaliser and investigate when the normaliser splits as a direct product.

We carry out a similar investigation for normalisers of cyclic subgroups of A_n and investigate the relationship between normalisers in A_n and S_n.

We give presentations for both centralisers and normalisers.

Notation

Number theory

(m, n)	highest common factor of m and n
$\text{lcm}(m, n)$	least common multiple of m and n
$\phi(n)$	The Euler ϕ–function.

Group Theory

x^g	conjugate of x by g, i.e. $g^{-1}xg$, where $x, g \in G$
$[x, y]$	the commutator of x with y, i.e. $x^{-1}y^{-1}xy$
$\|g\|$	order of the element g
$1, id$ or 1_G	the identity of the (multiplicative) group G
H^G	the normal closure of H in G
k^h	the action of h on k with $h \in H, k \in K$
$g\phi$	the image of g under ϕ
1_G	the identity map of the group G
C_n	cyclic group of order n
$S(\Omega)$ or S_Ω	symmetric group on the set Ω
S_n	symmetric group of degree n
$A(\Omega)$ or A_Ω	alternating group on the set Ω
A_n	alternating group of degree n
D_n	dihedral group of order $2n$

$\mathbb{Z}_m$	the ring of integers under addition and multiplication modulo m
$U(\mathbb{Z}_m)$ or U_m	the group of units in $\mathbb{Z}_m$ under multiplication
$G = H \ltimes K$	G is an internal semidirect product of K by H with $K \lhd G$
$H \,{}_\phi\!\times K$	external semidirect product of K by H with action ϕ
$G \wr H$	a wreath product of G by H
$C_G(g)$	centraliser of the element g in G
$C_G(H)$	centraliser of the subgroup H in G
$N_G(H)$	normaliser of subgroup H in G
$Z(G)$	centre of the group G
$\langle x_1, x_2, \ldots, x_n \rangle$	subgroup generated by the set $\{ x_1, x_2, \ldots, x_n \}$
$\langle H, K \rangle$	the subgroup generated by the union $H \cup K$
$(a_1, a_2, \ldots, a_k)$	a cycle of length k. We choose this non-standard notation (with commas) since this is the way GAP package represents them.
$[a_1, a_2, \ldots, a_k]$	the ordered set. (Again this is non-standard, since we have used the more usual notation for cycles)
$\mathrm{Aut}(\Gamma)$	automorphism group of the graph Γ
$\langle X \mid R \rangle$	group presentation with generating set X and defining relations R

Chapter 1

Preliminary Discussion and Definitions

1.1 Introduction

In this chapter we introduce some terminology, notation and some well known results from areas of group theory to be used in this work. Other definitions and results will be introduced when needed. For these definitions and proofs of some theorems see the books on group theory given in the bibliography, especially Rose [16, Chapter 9]. We also give a brief introduction to GAP.

The result that the centraliser of a permutation in the symmetric group can be considered as a direct product of wreath products has been noted several times, see Suzuki [19, Chapter 3, Section 2] and Wells [20]. In this thesis we examine the more general problem of analysing the structure of the normaliser of the cyclic subgroup generated by such a permutation.

As in the centraliser case, we are able to reduce the problem to looking at regular permutations (those which are the disjoint product of cycles of the same

length). The structure that we find is more complicated than the straightforward wreath products obtained for the centraliser, but it can still be represented as a semidirect product.

We are able to show that in certain cases, the groups obtained break up as direct products and we are able to obtain necessary and sufficient conditions for this to happen.

We also consider the corresponding problem for the centraliser and normaliser of a permutation in the subgroup A_n of even permutations. In this case we can also reduce the problem to that of a regular permutation and show how the centraliser is either a wreath product or a different semidirect product. The structure of the normaliser of a cyclic subgroup in A_n is also analysed. We prove an interesting theorem about the action of the automorphism group of a cyclic group and using this result we are able to give a classification of the normalisers in all the different possible cases.

We analyse the way in which the centralisers and the normalisers in S_n and A_n are connected.

Extensive use of computer experiment was made in the discoveries mentioned above. The GAP package (see Section 1.6 and Chapter 6) was used to investigate many special cases and then the general theorems were developed from these results. In some cases, the computer analysis also gave clues to how the theorems could be proved.

1.2 Elementary Group Theory

Definition 1.2.1 Let x, g be elements of a group G. Then the element $g^{-1}xg$ is called the **conjugate of x by g** and is sometimes denoted by x^g.

Definition 1.2.2 Let g, h be elements of a group G. Then they are called **conjugate** if there exists $x \in G$ such that $x^{-1}gx = h$. In this case we say that x conjugates g into h.

Definition 1.2.3 If H and K are groups, then the **external direct product** of H and K, denoted by $H \times K$, is the set of all ordered pairs (h, k), where $h \in H$ and $k \in K$, with the binary operation

$$(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2).$$

Definition 1.2.4 A group G is said to be the **internal direct product** of H and K if G contains subgroups H and K such that

(i) $H \lhd G$ and $K \lhd G$,

(ii) $HK = G$,

(iii) $H \cap K = \{1\}$.

Definition 1.2.5 Let H be a subgroup of a group G. The **normal closure** of H in G is defined to be the intersection of all normal subgroups of G which contain H, and is denoted by H^G. Then one can show that

(i) H^G is the unique smallest normal subgroup of G containing H,

(ii) $H^G = \langle g^{-1}hg : g \in G, h \in H \rangle$.

1.3 Semidirect Products

Definition 1.3.1 A group G is an **internal semidirect product** of K by H, denoted by $H \ltimes K$, if G contains subgroups K and H such that

(i) $K \lhd G$,

(ii) $HK = G$,

(iii) $K \cap H = \{1\}$.

Remark 1.3.2 We have the following exact sequence

$$1 \longrightarrow K \xrightarrow{i} G \underset{s}{\overset{\pi}{\rightleftarrows}} G/K \longrightarrow 1$$

where i is the inclusion map, π is the projection onto the quotient and s is a map (called a section) from the quotient to the subgroup H of G satisfying

$$s\pi = 1_{G/K}.$$

The image of s in G is the subgroup H. This exhibits the semidirect product as a split extension.

Definition 1.3.3 Let H and K be groups. We say that $\boldsymbol{H}$ **acts on** $\boldsymbol{K}$ (as a group) if, to each $h \in H$ and $k \in K$, there corresponds a unique element $k^h \in K$ such that, for all $k, k_1, k_2 \in K$ and $h, h_1, h_2 \in H$,

(i) $(k^{h_1})^{h_2} = k^{h_1 h_2}$,

(ii) $k^1 = k$ where 1 is the identity of H,

(iii) $(k_1 k_2)^h = {k_1}^h {k_2}^h$.

Theorem 1.3.4 Let H act on K. Then to each $h \in H$ there corresponds a map $\varphi_h : K \longrightarrow K$, defined by $\varphi_h : k \longmapsto k^h$, and this is an automorphism of K. Moreover the map, $\varphi : H \longrightarrow \mathrm{Aut}(K)$, defined by $\varphi : h \longmapsto \varphi_h$, is a homomorphism. We call φ the **automorphism representation** of H corresponding to the action, or, more frequently, we simply call φ the **action**.

Theorem 1.3.5 Let φ be a homomorphism of H into $\mathrm{Aut}(K)$. Then H acts on K when we define, for each $h \in H$ and $k \in K$,

$$k^h = k(h\varphi),$$

and the corresponding action is φ.

Theorem 1.3.6 Let H act on K, say with action φ. Then the set of all ordered pairs (h, k) acquires the structure of a group G when we define:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, {k_1}^{h_2} k_2). \tag{1.1}$$

This group is called **the external semidirect product of K by H with action φ** and denoted by $G = H \,{}_{\varphi}\!\times K$.

Theorem 1.3.7 Let H act on K with action φ. Let $G = H \,{}_{\varphi}\!\times K$. Let H_1 be the subset of G given by $\{\,(h, 1_K) \mid h \in H\,\}$ and let K_1 be the subset of G given by $\{\,(1_H, k) \mid k \in K\,\}$. Then $H \cong H_1 \leqslant G$, $K \cong K_1 \lhd G$, $G/K_1 \cong H_1$, $G = H_1 K_1$ and $H_1 \cap K_1 = \{\,1\,\}$. Moreover the action of H_1 on K_1 is the restriction to H_1 of the action by conjugation of G on K_1.

Theorem 1.3.8 If G is a semidirect product of K by H, then $G \cong H \,{}_{\varphi}\!\times K$ for some $\varphi : H \longrightarrow \mathrm{Aut}(K)$ which corresponds to conjugation.

Proof:

Define $k\varphi_h = h^{-1}kh$. Now $h^{-1}kh \in K$ since K is normal. Since $G = HK$ each $g \in G$ has expression $g = hk$, where $h \in H$ and $k \in K$; this expression is unique because $H \cap K = \{\,1\,\}$. Multiplication in G satisfies:

$$(h_1 k_1)(h_2 k_2) = h_1 h_2 ({h_2}^{-1} k_1 h_2) k_2 = h_1 h_2 {k_1}^{h_2} k_2.$$

It is now easy to see that the map $H \,{}_{\varphi}\!\times K \longrightarrow G$ defined by $(h, k) \longmapsto hk$ is an isomorphism. $\square$

1.4 Permutation Groups

Let Ω be a finite set. Let $S(\Omega)$ (sometimes S_Ω) denote the set of all 1–1 mappings from Ω onto itself. Then $S(\Omega)$ is a group under the composition of mappings and is called the **symmetric group** acting on the set Ω. When $\Omega = \{1, 2, \ldots, n\}$, then $S(\Omega)$ is written as S_n and is called the **symmetric group of degree n**, or **the symmetric group on n symbols**. The elements of S_n are called **permutations** and any subgroup of S_n is called a **permutation group**. We can denote a permutation α of Ω by displaying its values:

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1\alpha & 2\alpha & \ldots & n\alpha \end{pmatrix}.$$

Thus,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

are permutations of $\{1, 2, 3, 4\}$. Their product is

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

(we compute this product by first applying α and then β). Some authors adopt the opposite convention, which is more appropriate when the image of j under β is denoted by $\beta(j)$ and not by $j\beta$. We will denote the image of j under β as $j\beta$ throughout this work.

By a cycle $(a_1, a_2, \ldots, a_m)$ of length m we mean the permutation that carries a_1 into a_2, a_2 into $a_3, \ldots,$ a_{m-1} into a_m, a_m into a_1. We put commas in our cycles since this corresponds to the notation in the GAP programming language. All 1-cycles equal the identity permutation, which we denote by (1) or id. Every

permutation can be uniquely written into disjoint cycles. For example:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = (1,2)(3,4,5)$$

and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1,2,3)(4)(5) = (1,2,3).$$

Any two cycles commute if they are disjoint, i.e, if there is no symbol that occurs in both. A cycle of length 2 is called a **transposition.** Any two permutations α and $\beta \in S_n$ are conjugate if and only if they have same cycle type; that is, if and only if the expression of α and β as products of disjoint cycles contain the same number of cycles of length m, for each m such that $1 \leqslant m \leqslant n$. A permutation $\alpha \in S_n$ is said to be **regular** if it is the identity or it has no fixed points and is the product of disjoint cycles of the same length.

Throughout this work we will generally refer to permutations by their cycle notations. Permutation groups in general are very important in the study of group theory. For example, we have the theorem proved by Cayley, 1878:

Theorem 1.4.1 (Cayley) Every group G is isomorphic to a subgroup of $S(G)$. In particular, every finite group of order n is isomorphic to a subgroup of S_n.

1.5 Permutation Wreath Products

Let H be a group acting on the finite set X with $|X| = k$. Let G be another group. Let G^* be the direct product of k copies of G. i.e. $G^* = G \times G \times \ldots \times G$ (k copies). As in Rose [16, Lemma 8.21, page 186], the elements of G^* are functions from X into G (written on the left of the elements of X to which they apply) with the binary operation:

$$(ff')(x) = f(x)f'(x); \quad f, f' \in G^*, x \in X.$$

Then H acts on G^* (as a group) when, for each $h \in H$ and $f \in G^*$, we define $f^h \in G^*$, for all $x \in H$, by

$$f^h(x) = f(xh^{-1}).$$

To see that the axioms of Definition 1.3.3 are satisfied, see the proof of Lemma 9.18 in Rose [16, page 219].

Now let φ denote the action of H on $G^* = G \times G \times \ldots \times G$ (k copies) defined above. Then the corresponding semidirect product $H \,{}_{\varphi}\!\times G^*$ of G^* with H is said to be **a wreath product of G by H**, denoted by $G \wr H$. The order of $G \wr H$ is $|G|^{|X|}|H|$.

Note that the elements of G^* can be identified with k-tuples $(g_1, g_2, \ldots, g_k)$ with each $g_i \in G$ and if H is a subgroup of the symmetric group S_k then the action of $h \in H$ on the elements of G^* is given by

$$(g_1, g_2, \ldots, g_k)^h = (g_{1h^{-1}}, g_{2h^{-1}}, \ldots, g_{kh^{-1}}). \tag{1.2}$$

Example 1.5.1 Let H be a permutation group acting on $X = \{1, 2, \ldots, k\}$, i.e. $H \leqslant S_k$, for some k. Let G be another group. Then the action of $h = (1, 2, 3) \in H$ on an element of $G \times \cdots \times G$ (k copies) is given by

$$(g_1, g_2, g_3, \ldots, g_k)^h = (g_3, g_1, g_2, \ldots, g_k).$$

Note that, if G is also a permutation group acting on a finite set Ω with $|\Omega| = m$, in order to get the direct product of k copies of G we take k disjoint copies of G and Ω, say $G_1, \ldots, G_k$ and $\Omega_1, \ldots, \Omega_k$ with G_i acting on Ω_i. Then we let $G_1 \times G_2 \times \cdots \times G_k$ act on $\Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_k$ in the obvious manner. An element of such a wreath product consists of an element of H and k elements of G and we will frequently use the notation

$$[h'; g'_1, g'_2, \ldots, g'_k] \quad \text{with } h' \in H \text{ and } g'_i \in G_i \tag{1.3}$$

to represent this element.

We are interested in the case where $H \leqslant S_k$ and $G \leqslant S_m$ for some k and m. In this case

$$X = \{1, 2, \ldots, k\} \quad \text{and} \quad \Omega = \{1, 2, \ldots, m\}$$

and the wreath product can be regarded as a subgroup of S_{mk}. We will regard blocks $\{\Omega_i\}$ as ordered sets we let

$$\begin{aligned}
\Omega_1 &= [1, 2, \ldots, m], \\
\Omega_2 &= [m+1, m+2, \ldots, 2m], \\
&\vdots \\
\Omega_k &= [(k-1)m+1, (k-1)m+2, \ldots, km].
\end{aligned}$$

Thinking of it in this way, we get the internal wreath product $G \wr H$ in S_{mk} in the following way. We define the permutation in S_{mk} corresponding to $g'_i \in G_i$ to be the permutation acting on Ω_i and denote it by g_i. Similarly we use the notation h to mean the permutation in S_{mk} corresponding to $h' \in H$ and we define it in the following way. If $h' \in H$ maps the symbol x into the symbol y then the permutation $h \in S_{mk}$ maps the i-th symbol of Ω_x into Ω_y for every i with $1 \leqslant i \leqslant m$. In this case the permutation $h \in S_{mk}$ will permute the Ω_i among themselves. So h acts on blocks in the same as h' acts on Ω.

In (1.2) when, say $g_{1h^{-1}}$, is moved to g_1 then since the first copy of G acts on Ω_1 we replace it with the corresponding element of G acting on Ω_1 rather than the one acting on $\Omega_{1h^{-1}}$. By the construction, conjugation by $h \in S_{mk}$ corresponds to action given in (1.2).

Example 1.5.2 Let $G = \langle (1,2,3,4) \rangle \cong C_4$ and $H = \langle (1,2,3,4,5), (1,2) \rangle \cong S_5$. Then the wreath product of G by H is the group acting on 20 symbols. Here

$$\begin{aligned} \Omega_1 &= [1,2,3,4], & \Omega_2 &= [5,6,7,8], \\ \Omega_3 &= [9,10,11,12], & \Omega_4 &= [13,14,15,16] \\ \Omega_5 &= [17,18,19,20]. \end{aligned}$$

The permutation $h_1 = (1,2,3,4,5)$ acting on the Ω_i then corresponds to

$$\gamma = (1,5,9,13,17)(2,6,10,14,18)(3,7,11,15,19)(4,8,12,16,20)$$

while the permutation $h_2 = (1,2)$ corresponds to

$$\beta = (1,5)(2,6)(3,7)(4,8).$$

We will see later that

$$G \wr H = \langle (1,2,3,4), \beta, \gamma \rangle.$$

The order of this group is $122880 = 5! \cdot 4^5$.

We let $\alpha_i = (4i-3, 4i-2, 4i-1, 4i)$ be the generator for the i-th copy of C_4 for $1 \leqslant i \leqslant 5$. Then the element $x = (g_1, {g_2}^2, {g_3}^3, {g_4}^3, {g_5}^2)$ corresponds to

$$\rho = (1,2,3,4)(5,7)(6,8)(9,12,11,10)(13,16,15,14)(17,19)(20,21)$$

and the element $h = (1,2,3)$ acting on Ω_i corresponds to

$$\pi = (1,5,9)(2,6,10)(3,7,11)(4,8,12).$$

If we conjugate ρ with π we get

$$\pi^{-1}\rho\pi = (1,4,3,2)(5,6,7,8)(9,11)(10,12)(13,16,15,14)(17,19)(20,21).$$

This element corresponds to $({g_1}^3, g_2, {g_3}^2, {g_4}^3, {g_5}^2)$. We let

$$x = (g_1, {g_2}^2, {g_3}^3, {g_4}^3, {g_5}^2) = (t_1, t_2, t_3, t_4, t_5).$$

Now we have

$$\begin{aligned} x^h = (t_1, t_2, t_3, t_4, t_5)^h &= (t_{1h^{-1}}, t_{2h^{-1}}, t_{3h^{-1}}, t_{4h^{-1}}, t_{5h^{-1}}) \\ &= (t_3, t_1, t_2, t_4, t_5) \\ &= ({g_1}^3, g_2, {g_3}^2, {g_4}^3, {g_5}^2) \end{aligned}$$

which corresponds to ${\alpha_1}^3\alpha_2\alpha_3{}^2{\alpha_4}^3{\alpha_5}^2$ in S_{20}. In the previous equation, for example, when $t_3 = {g_3}^3$ comes to the first place we replace it with the corresponding element acting on Ω_1 (i.e. ${g_1}^3$), which corresponds to ${\alpha_1}^3$.

Remark 1.5.3 From the definition of the multiplication in the wreath product, (see (1.1)), for

$$\tau_1 = [h; g_1, g_2, \ldots, c_k] \quad \text{and} \quad \tau_2 = [h'; g_1', g_2', \ldots, g_k']$$

we must have

$$\tau_1\tau_2 = [hh'; g_{1h^{-1}}g_1', \ldots, g_{kh^{-1}}g_k'].$$

Remark 1.5.4 If, for example, $1h^{-1} = 4$ when we calculate $g_{1h^{-1}}$ we must take the element corresponding to $g_4 \in G$, but acting on the elements of the first block rather than the fourth.

We illustrate this with:

Example 1.5.5 Let $G = \langle (1,2,3) \rangle \cong C_3$ and $H = \langle (1,2,3,4), (1,2) \rangle \cong S_4$. As in the previous example we define α_i's and Ω_i's. Let

$$\tau_1 = [(1,2)(3,4); c_1, id, {c_3}^2, c_4] \quad \text{and} \quad \tau_2 = [(1,2,3,4); c_1, c_2, {c_3}^2, id].$$

where $(1,2)(3,4)$ and $(1,2,3,4)$ represent the permutations of blocks and the c_i's are the generators of the copies of C_3. Then we have:

$$h = (1,2)(3,4), \quad g_1 = c_1, \quad g_2 = id, \quad g_3 = {c_3}^2, \quad g_4 = c_4,$$
$$h' = (1,2,3,4), \quad g'_1 = c_1, \quad g'_2 = c_2, \quad g'_3 = {c_3}^2, \quad g'_4 = id.$$

Then,

$$\begin{aligned}\tau_1\tau_2 &= [(1,2)(3,4)(1,2,3,4); g_4g'_1, g_1g'_2, g_2g'_3, g_3g'_4] \\ &= [(1,3); c_1c_1, c_2c_2, id\ {c_3}^2, {c_4}^2\ id] \\ &= [(1,3); {c_1}^2, {c_2}^2, {c_3}^2, {c_4}^2].\end{aligned}$$

We may calculate that the permutation corresponding to the element

$$[(1,3); {c_1}^2, {c_2}^2, {c_3}^2, {c_4}^2]$$

is $(1,9,2,7,3,8)(4,6,5)(10,12,11)$ which is $\tau_1\tau_2$.

Remark 1.5.6 One may get an alternative view of a permutation wreath product as a generalisatin of a block-design in the paper by Bailey et al. [2].

Remark 1.5.7 For abstract groups G and H we define the wreath product corresponding to the action of H on itself by right multiplication. In this case the elements of H take the place of the symbols in X. Then the wreath product will have order $|G|^{|H|}|H|$. This is called the **regular wreath product**.

Throughout this thesis, all wreath products are defined in terms of permutation wreath products.

1.6 The GAP Package

With the widespread introduction of computers, computer programs in algebra are playing a more important role in the study of group theory. In 1936 Todd and Coxeter converted a technique, introduced by E.H.Moore (1897) and others into a procedure to compute the index of a subgroup in a given finitely presented group. This was later implemented on a computer. Since then, many programs have appeared. These programs help the algebraist to study more problems in group theory. In 1988 the programming language GAP, specially designed to handle algebraic problems, appeared. The word GAP stands for "Groups, Algorithms and Programming". It started as a joint project of a group of students in Aachen, among whom were Johannes Meier, Werner Nickel, Alice Niemeyer and Martin Schönert, in 1985. The system was first presented outside Aachen in 1988 and has been developed to Version 3.4 Release 4 by 1997.

It is implemented by having a small kernel written in C which then calls routines from modules which can be written by any other user. Because of this design and the fact that GAP can be run on most major operating systems, work done by one user can be exploited and developed by others.

The GAP package includes a set of standard modules. Modules written by other users are available freely as **share libraries** from internet sites such as `http://www-gap.dcs.st-andrews.ac.uk/~gap`. The GAP operational manual can be viewed in HTML form at this site. The GAP Forum is a mailing list for the discussion of problems relating to GAP and the archives of this forum are also available at the `st-andrews` site.

We have used GAP for our research and most of the results have been motivated by experiments in GAP.

Chapter 2

Centralisers in S_n

2.1 Introduction

The centraliser of an element g in a group G, denoted by $C_G(g)$, is the set of elements which commute with g. Thus

$$C_G(g) = \{ x \in G \mid gx = xg \} = \{ x \in G \mid x^{-1}gx = g \}.$$

It is easy to verify that $C_G(g)$ is a subgroup of G.

The centraliser of a subgroup H in G is the set of elements of G which commute with each element of H, and is denoted by $C_G(H)$. That is

$$C_G(H) = \{ x \in G \mid x^{-1}hx = h \text{ for all } h \in H \}.$$

As before, $C_G(H)$ is always a subgroup of G. Note that if $H = \langle g \rangle$ then $C_G(H) = C_G(g)$.

It is known that the centraliser of a permutation σ in S_n is the direct product of centalisers of regular permutations and that the centraliser of a regular permutation is a wreath product (see Suzuki [19, Chapter 3, Section 2] and Wells [20]). In this chapter we examine the structure of this wreath product and show that it

can be written as a direct product in certain cases. We also examine the structure of these direct summands. We give some applications of the wreath product construction to symmetries of geometric figures and to automorphism groups of certain graphs. Some of these applications have been examined in Wells [20], Hoffmann [6] and Harary [4, 5]. We also give a presentation for the wreath product which arises as the centraliser of a regular permutation.

2.2 Centralisers of Elements in S_n

In a permutation group S_n any two permutations with the same cycle structure are conjugate. Conjugating an element in S_n gives a permutation with the same cycle shape. For example to find an element $\rho \in S_5$ which conjugates $\sigma = (1,2,3)(4,5)$ into $\tau = (2,3,5)(1,4)$ we have the following diagram:

$$\left.\begin{array}{rcccc} \sigma & = & (1,2,3) & (4,5) \\ & & \Downarrow & \Downarrow \\ \tau & = & (2,3,5) & (1,4) \end{array}\right\} \Longrightarrow \rho = (1,2,3,5,4)$$

$$(1,2,3,5,4)^{-1}\underbrace{(1,2,3)(4,5)}_{\sigma}(1,2,3,5,4) = \underbrace{(2,3,5)(1,4)}_{\tau}.$$

If two cycles are of the same length, e.g.:

$$\begin{array}{rcl} \sigma & = & (1,2,3)(4,5,6) \\ & & \swarrow\!\!\!\searrow \\ \tau & = & (\bullet\ \bullet\ \bullet)(\bullet\ \bullet\ \bullet) \end{array}$$

then we can swap them:

$$\left.\begin{array}{rcccc} \sigma & = & (1,2,3) & (4,5,6) \\ & & \Downarrow & \Downarrow \\ \tau & = & (4,6,5) & (3,1,2) \end{array}\right\} \Longrightarrow (1,4,3,5)(2,6).$$

In particular, if $\sigma = \tau$ then we can use this method to produce an element in the centraliser of σ, i.e. such that $\rho^{-1}\sigma\rho = \sigma$. e.g.

$$\left.\begin{array}{rcl} \sigma & = & (1,2,3)(4,5,6) \\ & & \Downarrow \\ \sigma & = & (4,5,6)(3,1,2) \end{array}\right\} \Longrightarrow \rho = (1,4,3,6,2,5).$$

$$\left.\begin{array}{rcll} \sigma & = & (1,2,3)(4,5,6) & (7,8)(9,10) \\ & & \Downarrow & \Downarrow \\ \sigma & = & (5,6,4)(3,1,2) & (8,7)(9,10) \end{array}\right\} \Longrightarrow \rho = (1,5)(2,6)(3,4)(7,8).$$

Now assume $\sigma = \ldots(a,b,c)(d,e,f)(g,h,i)\ldots \in S_n$, and these are the only 3-cycles in the representation of σ as a product of disjoint cycles. Assume $\tau^{-1}\sigma\tau = \sigma$. Now, what choice do we have in conjugating?

$$\left.\begin{array}{rcl} \sigma & = & \ldots(a,b,c)(d,e,f)(g,h,i)\ldots \\ & & \Downarrow \tau \\ \sigma & = & \ldots(\bullet\ \bullet\ \bullet)(\bullet\ \bullet\ \bullet)(\bullet\ \bullet\ \bullet)\ldots \end{array}\right\}$$

Since conjugating by τ gives something with the same shape, the image of first 3-cycle under τ is a 3-cycle contained in the disjoint decomposition of σ. Therefore $(a\tau, b\tau, c\tau)$ is one of the $(\bullet\ \bullet\ \bullet)$'s. Let's say it is the first one.

$$\left.\begin{array}{rcl} \sigma & = & \ldots(a,b,c)(d,e,f)(g,h,i)\ldots \\ & & \Downarrow \tau \\ \sigma & = & \ldots(a,b,c)(\bullet\ \bullet\ \bullet)(\bullet\ \bullet\ \bullet)\ldots \end{array}\right\}$$

Note that, we can permute the symbols in any cycle cyclically. e.g. instead of (a,b,c) we can write (b,c,a) or (c,a,b). When we write the cycles we get new elements to conjugate by. We can also write (a,b,c) under any 3-cycle, that is, we can permute "blocks" in any way we like, as long as we permute them among those which have the same cycle length e.g.

$$\left.\begin{array}{rcl} \sigma & = & \ldots(a,b,c)(d,e,f)(g,h,i)\ldots \\ & & \Downarrow \tau \\ \sigma & = & \ldots(h,i,g)(b,c,a)(d,e,f)\ldots \end{array}\right\} \Longrightarrow \tau = (a,h,e,c,g,d,b,i,f).$$

We will see later that this gives us the structure of a wreath product. In this

example we get the wreath product of a cyclic group C_3 by the symmetric group S_3.

We can reduce the problem of identifying the centraliser to looking at the direct product of groups for each cycle length. For example:

$$C_{S_{10}}\big((1,2,3)(4,5,6)(7,8)(9,10)\big) \cong C_{S(\Omega_3)}\big((1,2,3)(4,5,6)\big) \times C_{S(\Omega_2)}\big((7,8)(9,10)\big),$$

where $\Omega_3 = \{1,2,3,4,5,6\}$ and $\Omega_2 = \{7,8,9,10\}$.

We have the following result:

Theorem 2.2.1 Let $\sigma \in S_n$. Assume that σ is written as a product of disjoint cycles. Let σ_{m_i} be the product of all m_i-cycles in σ (provided there is at least one m_i-cycle). Let Ω_{m_i} be the set of symbols on which σ_{m_i} acts and let r be the number of different cycle lengths in σ. If σ leaves some symbols fixed then we may regard the product of 1-cycles in the disjoint cycle representation of σ as a regular permutation σ_1 acting as the identity on a set Ω_1. (In this case the centraliser of σ_1 on this set will be the whole of $S(\Omega_1)$.) Then

$$C_{S_n}(\sigma) \cong C_{S(\Omega_{m_1})}(\sigma_{m_1}) \times C_{S(\Omega_{m_2})}(\sigma_{m_2}) \times \ldots \times C_{S(\Omega_{m_r})}(\sigma_{m_r}).$$

Proof:

Let $\rho \in C_{S_n}(\sigma)$, so that $\rho^{-1}\sigma\rho = \sigma$. We have $\sigma = \sigma_{m_1} \cdot \sigma_{m_2} \cdot \ldots \cdot \sigma_{m_r}$. Since σ_{m_i} and σ_{m_j} are products of cycles of different length for $i \neq j$, then $\rho_{m_1} = \rho|\Omega_{m_1}$ maps into Ω_{m_1} and conjugates σ_{m_1} into itself. Similarly, we have $\rho_{m_2}, \rho_{m_3}, \ldots, \rho_{m_r}$ which conjugate $\sigma_{m_2}, \sigma_{m_3}, \ldots, \sigma_{m_r}$ into themselves. It is easy to see that $\rho_{m_1}, \rho_{m_2}, \ldots, \rho_{m_r}$ commute with each other, since they act on disjoint sets. This shows that:

$$C_{S_n}(\sigma) \subseteq C_{S(\Omega_{m_1})}(\sigma_{m_1}) \times C_{S(\Omega_{m_2})}(\sigma_{m_2}) \times \ldots \times C_{S(\Omega_{m_r})}(\sigma_{m_r}).$$

Conversely, if we have $\rho_i \in S(\Omega_{m_i})$ with $\rho_i^{-1}\sigma_{m_i}\rho_i = \sigma_{m_i}$ then it is clear that the product $\rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_r$ conjugates σ into σ. Hence the result follows. □

Example 2.2.2 Let $\sigma = (1,2)(3,4,5)(6,7)(8,9,10,11) \in S_{14}$. Then,

$$C_{S_{14}}(\sigma) \cong C_{S(\Omega_2)}\big((1,2)(6,7)\big) \times C_{S(\Omega_3)}\big((3,4,5)\big) \times C_{S(\Omega_4)}\big((8,9,10,11)\big) \times S(\Omega_1).$$

where

$\Omega_1 = \{12,13,14\}$,

$\Omega_2 = \{1,2,6,7\}$,

$\Omega_3 = \{3,4,5\}$, and

$\Omega_4 = \{8,9,10,11\}$.

We have proved that the centraliser of a permutation in a symmetric group is a direct product. Each component in this direct product is the centraliser of a regular permutation, which we will prove to be a wreath product.

2.3 Centralisers of Regular Permutations

We begin this section by examining an example.

Example 2.3.1 Let $\sigma = (1,2,3)(4,5,6)(7,8,9)(10,11,12) \in S_{12}$. We are trying to find τ with $\tau^{-1}\sigma\tau = \sigma$. Then we have the following figure:

$$\left.\begin{array}{rcccccc} \sigma & = & (1,2,3) & (4,5,6) & (7,8,9) & (10,11,12) \\ & & \Downarrow & \Downarrow & \Downarrow & \Downarrow \\ \sigma & = & (\bullet\ \bullet\ \bullet) & (\bullet\ \bullet\ \bullet) & (\bullet\ \bullet\ \bullet) & (\bullet\ \bullet\ \bullet) \end{array}\right\}$$

Notice that, since $\tau \in C_{S_{12}}(\sigma)$ conjugates a 3-cycle into itself or into another 3-cycle, then $(1,2,3)$ is one of the $(\bullet\ \bullet\ \bullet)$'s. Therefore the bottom line is a rearrangement of blocks. Notice also that when writing a 3-cycle, say $(1,2,3)$, we can start from 1, 2 or 3, that is to say, we can permute the symbols in a block cyclically. We have $4! = 24$ permutations of blocks and, for each permutation of blocks we have $3^4 = 81$ permutations inside the blocks. So the number of different τ we can get is 1944. We will show later that this gives us the structure of a wreath product: in this case

$$C_3 \wr S_4 = S_4 \ltimes \left(C_3 \times C_3 \times C_3 \times C_3\right)$$

which has order $3^4 \cdot 4! = 1944$. (See Section 1.5.)

Theorem 2.3.2 Let σ be a regular permutation which is a product of k disjoint m-cycles. The centraliser of σ in S_{mk} is a wreath product $C_m \wr S_k$.

Proof:

We suppose that σ is a product of m-cycles where the i-th m-cycle permutes a set Ω_i. We take the i-th m-cycle as a generator for the i-th cyclic group. Suppose τ commutes with σ. Then τ conjugates σ into itself and so maps each set Ω_i into another such set. Thus τ defines a permutation h on the set $\{\Omega_i\}$ of blocks. As

above we choose for the permutation of S_{mk} corresponding to h, a permutation which permutes blocks. We shall show that τ can be written as

$$[h; c_1, c_2, \ldots, c_k]$$

in the notation of Section 1.5. To find a particular c_i we perform the following process. We let $c_i = (h^{-1}\tau)|_{\Omega_i}$. Then we have $i(h \cdot c_1 \ldots c_k) = i\tau$ for all $i \in \{1, \ldots, mk\}$ so $h \cdot c_1 \ldots c_k = \tau$. As $\Omega_i h = \Omega_i \tau$, by definition, it follows that $(\Omega_i h^{-1})\tau = \Omega_i$. Hence $c_i = (h^{-1}\tau)|_{\Omega_i}$ is a permutation of Ω_i. Furthermore as σ commutes with τ we have $[\Omega_j]\tau = [\Omega_i]'$, where $[\Omega_i]'$ is a cyclic permutation of $[\Omega_i]$, for some j. By definition $[\Omega_j]h = [\Omega_i]$ and so $[\Omega_i]c_i = [\Omega_j]\tau = [\Omega_i]'$. It follows that c_i is a power of the generator of C_i.

Conversely, any permutation which is an element of $C_m \wr S_k$ will commute with σ, and so we have a one-one correspondence. □

Remark 2.3.3 The above result together with Theorem 2.2.1 gives a description of the centraliser of an element in S_n as a direct product of wreath products. This result has been noted several times before e.g. Humphreys [7, Chapter 19] for the case $m = 2$, Suzuki [19, Chapter 3, Section 2]. Generalisations of this result for semigroups have been attempted in Lipscomb [13].

We illustrate this theorem with some examples.

Example 2.3.4 Let $\sigma = (1,2,3,4)(5,6,7,8)(9,10,11,12) \in S_{12}$. Then the centraliser of σ is isomorphic to $C_4 \wr S_3$ and we assume that the i-th copy of C_4 is generated by c_i for $i = 1, 2, 3$. In S_{12} the generators for the three copies of C_4 are choosen to be

$$\alpha_1 = (1,2,3,4), \quad \alpha_2 = (5,6,7,8), \quad \alpha_3 = (9,10,11,12).$$

A permutation in S_3 which swaps Ω_1 and Ω_2 corresponds to the element in S_{12}:

$$(1,5)(2,6)(3,7)(4,8).$$

The element $(c_1, {c_2}^2, {c_3}^3)$ viewed as an element of S_{12} is written as

$$(1,2,3,4)(5,7)(6,8)(9,12,11,10).$$

Let $h' = (1,2,3)$ be the element of S_3 which acts on blocks. Then in S_{12} this element corresponds to $h = (1,5,9)(2,6,10)(3,7,11)(4,8,12)$. Then in S_{12} the element

$$\tau = [h'; c_1, {c_2}^2, {c_3}^3]$$

corresponds to the permutation

$$\begin{aligned}&(1,5,9)(2,6,10)(3,7,11)(4,8,12)\cdot(1,2,3,4)(5,7)(6,8)(9,12,11,10)\\ &=(1,7,10,3,5,12)(2,8,11,4,6,9).\end{aligned}$$

The same element can be found using the diagram as follows: from the block permutation $h' = (1,2,3)$ we place the second block under the first block, the third block under the second block and the first block under the third block. The in-block permutation $(c_1, {c_2}^2, {c_3}^3)$ tells us that the first block is shifted once, the second block is shifted twice and the third block is shifted three times. The following emerges.

$$\left.\begin{array}{rcccc}\sigma &=& (1,2,3,4) & (5,6,7,8) & (9,10,11,12)\\ & & \Downarrow & \Downarrow & \Downarrow\\ \sigma &=& (7,8,5,6) & (12,9,10,11) & (2,3,4,1)\end{array}\right\} \Longrightarrow \begin{array}{l}\tau = (1,7,10,3,5,12)\\ (2,8,11,4,6,9).\end{array}$$

Remark 2.3.5 A block permutation tells us how these blocks are written under each other when calculating τ and c_i tells us how many times the i-th block is shifted when writing it down. For example, let

$$\sigma = (1,2,3)(4,5,6)(7,8,9)(10,11,12).$$

Let τ be the element of $C_{S_{12}}(\sigma)$

$$\tau = [(1,3,2); (id), c_2, {c_3}^2, (id)]$$

where $(1,3,2)$ represents the permutation of blocks and we assume the i-th copy of C_3 is generated by c_i. The permutation in S_{12} which corresponds to $h' = (1,3,2)$ is

$$h = (1,7,4)(2,8,5)(3,9,6).$$

This tells us that the third block is written under the first one, the second block is written under the third one and the first block is written under the second one. Also the first and the fourth blocks are written as $(1,2,3)$ and $(10,11,12)$ while the second and the third blocks are written as $(5,6,4)$ and $(9,7,8)$. So τ is

$$\left.\begin{array}{rcl} \sigma & = & (1,2,3)(4,5,6)(7,8,9)(10,11,12) \\ & & \Downarrow \\ \sigma & = & (9,7,8)(1,2,3)(5,6,4)(10,11,12) \end{array}\right\} \Longrightarrow \tau = (1,9,4)(2,7,5)(3,8,6).$$

Calculating the permutation which corresponds to τ in S_{12} we get

$$\underbrace{(1,7,4)(2,8,5)(3,9,6)}_{h} \cdot \underbrace{(4,5,6)}_{\alpha_2} \cdot \underbrace{(7,9,8)}_{{\alpha_3}^3} = (1,9,4)(2,7,5)(3,8,6).$$

where α_i is the permutation corresponding to c_i. □

Now we give an example illustrating how to find $h' \in S_k$ and c_i's when $\tau \in C_{S_{mk}}(\sigma)$ is given.

Example 2.3.6 Let $\sigma = (1,2,3)(4,5,6)(7,8,9)(10,11,12)$. Then

$$\tau = (1,4,2,5,3,6)(7,11)(8,12)(9,10)$$

is an element of $C_{S_{12}}(\sigma)$. It is easy to see here that the block transformation is $(1,2)(3,4)$. To find the c_i's we have

$$\begin{aligned} \tau &= (1,4,2,5,3,6)(7,11)(8,12)(9,10) \\ &= \underbrace{(1,4)(2,5)(3,6)(7,10)(8,11)(9,12)}_{h}\underbrace{(1,2,3)}_{\alpha_1}\underbrace{(id)}_{id}\underbrace{(7,9,8)}_{{\alpha_3}^2}\underbrace{(10,11,12)}_{\alpha_4} \\ &= [(1,2)(3,4); c_1, (id), {c_3}^2, c_4] \end{aligned}$$

where $(1,2)(3,4)$ represents block transformation. □

We continue this chapter by finding a generating set for the wreath product which arises as the centraliser of a regular permutation.

Let σ be a regular permutation in S_{mk}, say :

$$\sigma = (1,2,\ldots,m)(m+1,m+2,\ldots,2m)\ldots\big((k-1)m+1,\ldots,km\big).$$

Let σ_i be the i-th block for $i = 1,2,\ldots,k$. Then we have k copies of C_m in S_{mk}, namely the subgroups generated by σ_i's. We have a copy of S_k in S_{mk} which acts on blocks. Since the symmetric group S_k can be generated by the k-cycle $(1,2,\ldots,k)$ and the transposition $(1,2)$, this copy of S_k is generated by the permutations corresponding to the block permutations (Ω_1,Ω_2) and $(\Omega_1,\Omega_2,\ldots,\Omega_k)$. To find a generator set for $C_{S_{mk}}(\sigma)$ we take a generator from one copy of C_m and we take the generators for S_k. Therefore the following three permutations generate the centraliser.

$$\begin{aligned}
\alpha &= (1,2,\ldots,m),\\
\beta &= (1,m+1)(2,m+2)\ldots(m,2m),\\
\gamma &= \big(1,m+1,\ldots,(k-1)m+1\big)\ldots\big(m,2m,\ldots,km\big).
\end{aligned}$$

Here α represents the generator for the first copy of C_m. To obtain a generator of another copy of C_m we simply conjugate α with a suitable block permutation. For example in the previous example to obtain $(7,8,9)$ we conjugate $\alpha = (1,2,3)$ by $h = (1,7)(2,8)(3,9)$. That is

$$h^{-1}\alpha h = (7,8,9).$$

We now look in more detail at the structure of the wreath product.

First note that if A is an abelian group then in any wreath product $A \wr B$ with B a subgroup of S_k the "diagonal copy" of A in $A \times \cdots \times A$ given by

$$\{\,(a,a,\ldots,a) \mid a \in A\,\}$$

is a direct summand of $A \times \cdots \times A$ on which B acts trivially. In general, however, one cannot find another summand on which B acts. In the case $C_m \wr S_k$ that we have been considering, we can find another summand with an S_k-action in certain cases and then the diagonal copy of C_m will be a direct summand of the wreath product. Note that when we consider the wreath product $C_m \wr S_k$ as the centraliser of a regular permutation σ, the diagonal copy of C_m is the subgroup generated by σ. We have the following theorem.

Theorem 2.3.7 Let σ be a regular permutation which is a product of k disjoint m-cycles and let $G = C_m \wr S_k = C_{S_{mk}}(\sigma)$. Let H be the normal closure of S_k in G. Then

$$G \cong C_m \times H \quad \text{with } C_m = \langle \sigma \rangle$$

if and only if the highest common factor $(m, k) = 1$.

Proof:

Let σ_i be the i-th m-cycle in σ so that $\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$. Then as above, $S_k = \langle \beta, \gamma \rangle$ is generated by a k-cycle and a 2-cycle, and $G = \langle \sigma_1, \beta, \gamma \rangle$ (where $\alpha = \sigma_1$ in the above notation).

The normal closure H of S_k is generated by the set

$$\{ x, x^{\sigma_1}, x^{{\sigma_1}^2}, \ldots, x^{{\sigma_1}^{m-1}} \mid x \in S_k \}.$$

We will show that when k and m are coprime the whole group G can be generated by $\{ H, \sigma \}$. For this it is enough to write σ_1 in terms of H and σ. Now if $x \in S_k$ we have

$$x^{-1} x^{\sigma_1} = x^{-1} {\sigma_1}^{-1} x \sigma_1 = ({\sigma_1}^{-1})^x \sigma_1 = {\sigma_j}^{-1} \sigma_1 \in H$$

where $j = 1x^{-1}$. Conjugating by suitable elements of S_k gives all the elements of the form ${\sigma_i}^{-1} \sigma_j \in H$. Thus

$$\tau = {\sigma_k}^{-1} \sigma_1 {\sigma_{k-1}}^{-1} \sigma_1 \ldots {\sigma_2}^{-1} \sigma_1 \sigma_1 \sigma_2 \ldots \sigma_k \in \langle H, \sigma \rangle.$$

Since the σ_i's all commute, $\tau = {\sigma_1}^k$. Since σ_1 has order m, if k and m are coprime, some power of τ is σ_1 and thus $\sigma_1 \in \langle H, \sigma \rangle$ as required.

We define a subgroup T of G as follows:

$$T = \{\, x\ {\sigma_1}^{a_1} \cdots {\sigma_k}^{a_k} \mid x \in S_k,\ a_1 + \cdots + a_k \equiv 0 \pmod{m} \,\}.$$

We shall show that T is the normal closure H. To show that $T \lhd G$, let $\tau = x\ {\sigma_1}^{a_1} \cdots {\sigma_k}^{a_k}$ be an element of T and it will be enough to show that ${\sigma_1}^{-1}\tau\sigma \in T$. So we have

$${\sigma_1}^{-1}\tau\sigma_1 = ({\sigma_1}^{-1}x){\sigma_1}^{a_1} \cdots {\sigma_k}^{a_k}\sigma_1.$$

Since $x^{-1}{\sigma_1}^{-1}x = {\sigma_j}^{-1}$ with $j = 1x^{-1}$ we have

$${\sigma_1}^{-1}\tau\sigma_1 = x\ {\sigma_1}^{a_1+1} \cdots {\sigma_j}^{a_j-1} \cdots {\sigma_k}^{a_k} \in T.$$

Therefore $T \lhd G$. Since T contains S_k and H is the normal closure of S_k then we have $H \leqslant T$. It follows that

$${\sigma_1}^{a_1} \cdots {\sigma_k}^{a_k} \in H \Longrightarrow a_1 + \cdots + a_k \equiv 0 \pmod{m}.$$

Conversely let $a_1, \ldots, a_k$ be such that $a_1 + \cdots + a_k \equiv 0 \pmod{m}$. Then the element ${\sigma_1}^{a_1} \cdots {\sigma_k}^{a_k}$ can be written as

$$({\sigma_1}^{a_1}{\sigma_2}^{-a_1})({\sigma_2}^{a_1+a_2}{\sigma_3}^{-a_1-a_2}) \cdots ({\sigma_{k-1}}^{a_1+\cdots+a_{k-1}}{\sigma_k}^{-a_1-\cdots-a_{k-1}}){\sigma_k}^{a_1+\cdots+a_k}.$$

Since H includes all the elements of the form $\sigma_i{\sigma_j}^{-1}$ it follows that H includes all the elements of the form ${\sigma_i}^t{\sigma_j}^{-t}$ for every i, j. So the element ${\sigma_1}^{a_1} \cdots {\sigma_k}^{a_k}$ lies in H and we have $H = T$. We have just shown that all the elements of the form

$${\sigma_1}^{a_1} \cdots {\sigma_k}^{a_k} \quad \text{with} \quad a_1 + \cdots + a_k \equiv 0 \pmod{m}$$

can be written using $\{\, \sigma_i{\sigma_j}^{-1} \,\}$ and so we have $H = \langle \sigma_1{\sigma_2}^{-1}, \beta, \gamma \rangle$.

If $H \cap \langle \sigma \rangle \neq \{1\}$ then some power of σ lies in H. Since $(k, m) = 1$ it follows that $\sigma \in H$. But for σ the number $a_1 + \cdots + a_k = k$ and we must have

$k \equiv 0 \pmod{m}$. This is a contradiction since m and k are coprime. Hence $H \cap \langle \sigma \rangle = \{1\}$.

Clearly H is normal in G and so is $\langle \sigma \rangle$ and so we have a direct product.

If $(k, m) = d \neq 1$, then our argument shows that $\sigma^{\frac{m}{d}}$ lies in H and thus $H \cap \langle \sigma \rangle \neq \{1\}$ and so we do not have a direct product. □

Remark 2.3.8 The elements of the form $\sigma_i {\sigma_j}^{-1}$ generate an abelian subgroup, K (say), of H and we have shown that

$$K = \{ {\sigma_1}^{a_1} \dots {\sigma_k}^{a_k} \mid a_1 + \cdots + a_k \equiv 0 \pmod{m} \}.$$

The order of K is m^{k-1}. This subgroup is a subgroup of $\langle \sigma_1 \rangle \times \cdots \times \langle \sigma_k \rangle$ with index m. The group H is generated by $\langle S_k, K \rangle$ and K is fixed under the operation of S_k and so H is a semidirect product of K by S_k with order $k! m^{k-1}$ and thus has index m in G.

So $\langle \sigma \rangle$ and K are two subgroups of

$$\langle \sigma_1 \rangle \times \cdots \times \langle \sigma_k \rangle \cong C_m \times \cdots \times C_m.$$

If $(m, k) = 1$ then the intersection of these groups is trivial and $C_m \times \cdots \times C_m$ is their direct product. Note that K is the direct summand mentioned above immediately before the statement of Theorem 2.3.7.

Example 2.3.9 Let $\sigma \in S_{15}$ be the product of three 5-cycles, say

$$\sigma = (1,2,3,4,5)(6,7,8,9,10)(11,12,13,14,15).$$

Let σ_i be the i-th 5-cycle for $i = 1, 2, 3$. Let $Z = \langle \sigma \rangle$ and

$$\beta = (1,6)(2,7)(3,8)(4,9)(5,10) \text{ and}$$

$$\gamma = (1,6,11)(2,7,12)(3,8,13)(4,9,14)(5,10,15).$$

Then

$$G = C_{S_{15}}(\sigma) = \langle \sigma_1, \beta, \gamma \rangle.$$

We have a copy of S_3 in $C_{S_{15}}(\sigma)$ given by $\langle \beta, \gamma \rangle$. Now, let $H = {S_k}^G$. Then by Theorem 2.3.7

$$H = \langle \sigma_1 {\sigma_2}^{-1}, \beta, \gamma \rangle.$$

Again by Theorem 2.3.7, the elements in H of the form ${\sigma_1}^{a_1}{\sigma_2}^{a_2}{\sigma_3}^{a_3}$ satisfy

$$a_1 + a_2 + a_3 \equiv 0 \pmod 5.$$

Since $\sigma = \sigma_1\sigma_2\sigma_3$, the only power of σ which lies in H is id and so

$$Z \cap H = \{ id \}.$$

To show that $\langle H, Z \rangle = G$ we calculate:

$$\tau_1 = \sigma_1 {\sigma_2}^{-1} \sigma_1 {\sigma_3}^{-1} \cdot \sigma_1\sigma_2\sigma_3 = {\sigma_1}^3 \in \langle H, Z \rangle$$

so that ${\tau_1}^2 = \sigma_1 \in \langle H, Z \rangle$. Hence $G = \langle H, Z \rangle$. Since both H and Z are normal subgroups of G we have

$$\langle H, Z \rangle = HZ = G.$$

Example 2.3.10 Let $\sigma = (1,2,3,4)(5,6,7,8) \in S_8$. We use the same notation as in the previous example. In this case $G = C_{S_8}(\sigma)$ is a group of order 32 and $H = {S_2}^G$ has order 8 and is isomorphic to $\langle \sigma_1 {\sigma_2}^{-1}, \beta \rangle$. Notice that

$$\sigma_1 {\sigma_2}^{-1} \sigma_1 {\sigma_2}^{-1} = {\sigma_1}^2 {\sigma_2}^2 = \sigma^2.$$

Therefore $H \cap Z \neq \{ id \}$. In fact $H \cap Z = \langle \sigma^2 \rangle$. So G is not a direct product of H and Z. □

2.4 Some Results from Geometry and Graph Theory

In this section we present some applications of the wreath product construction to symmetries of geometrical figures and to automorphism groups of graphs. A good reference for automorphism groups of graphs is Harary [5]. Some results on the automorphism groups of graphs have been given in Hoffmann [6], Harary [4] and Wells [20].

We examine some simple cases.

Let $\sigma = (1,2)(3,4) \in S_4$. By Theorem 2.3.2 we see that $C_{S_4}(\sigma) \cong C_2 \wr S_2$ with order 8 and GAP result tells us that $C_{S_4}(\sigma)$ is not a direct product.

Let Γ be the graph of Figure 2.1.

Figure 2.1: A graph whose automorphism group is $C_2 \wr S_2$.

Then $C_{S_4}(\sigma) \cong \mathrm{Aut}(\Gamma)$. To see this, first we label vertices as in the figure. We see that $\mathrm{Aut}(\Gamma)$ acts on vertices. Then we have two copies of C_2, namely $\langle(1,2)\rangle$ and $\langle(3,4)\rangle$ and a copy of S_2 which swaps two line segments, i.e. $\langle(1,3)(2,4)\rangle$.

When we put these two line segments (of the same length) into separate dimensions we get the full symmetry group of a square, see Figure 2.2.

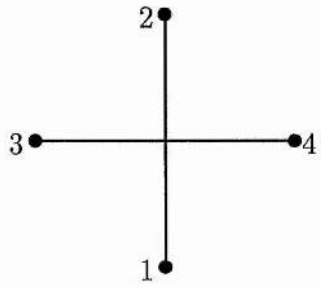


Figure 2.2: A figure whose symmetry group is $C_2 \wr S_2$.

Note that in this case the symmetry group is $D_4 \cong C_2 \wr S_2$ and is known not to be a direct product in accordance with Theorem 2.3.7.

Now let $\sigma = (1,2)(3,4)(5,6) \in S_6$. By Theorem 2.3.2 $C_{S_6}(\sigma) \cong C_2 \wr S_3$. This group is isomorphic to the automorphism group of the graph in Figure 2.3.

Figure 2.3: A graph whose automorphism group is $C_2 \wr S_3$.

Putting these three segments into three dimensions we get the figure in Figure 2.4. The symmetry group of this is the full symmetry group of the octahedron (or by duality, cube) and is the direct product of the rotation group of the octahedron (isomorphic to S_4) by the subgroup generated by central inversion, which is, of course just $\langle \sigma \rangle$.

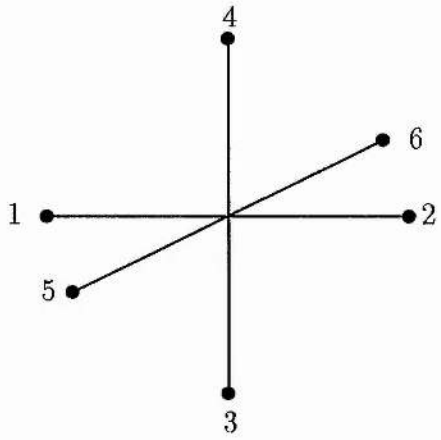


Figure 2.4: A three dimensional figure whose symmetry group is $C_2 \wr S_3$.

We now go one step further and we let $\sigma = (1,2)(3,4)(5,6)(7,8) \in S_8$. Theorem 2.3.2 and GAP results give us the following:

$$|C_{S_8}(\sigma)| = 384 \quad \text{and } C_{S_8}(\sigma) \text{ is not a direct product.}$$

As before, $C_2 \wr S_4$ is isomorphic to $\mathrm{Aut}(\Gamma)$ where Γ is the graph in Figure 2.5.

Figure 2.5: A graph whose automorphism group is $C_2 \wr S_4$.

And if we put these 4 line segments into different dimensions we get the group of a "16 cell". (See Coxeter [3, page 31].) Note that we may join the vertices in Figure 2.2 to get a square and the vertices in Figure 2.4 to get an octahedron. To get the 16-cell from the octahedron, we add two extra vertices which are then joined to the existing 6 vertices giving a polytope with 8 vertices (each with degree 6) and 24 edges. A representation of this is given in Figure 2.6.

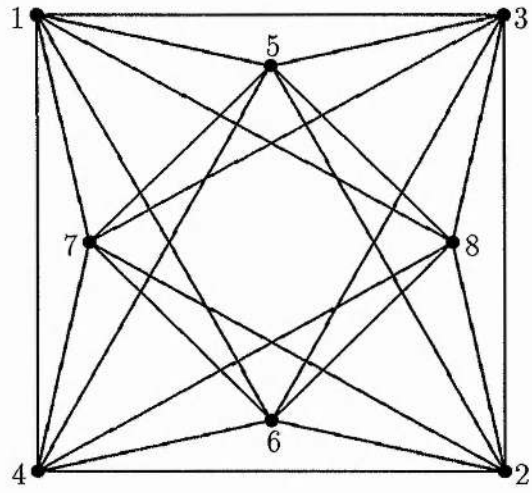


Figure 2.6: A two dimensional representation of a figure whose symmetry group is $C_2 \wr S_4$.

We now look at some graphs whose automorphism groups are $C_m \wr S_k$ with $m > 2$. We need to start with a graph whose automorphism group is C_m and unfortunately such graphs are rather complicated. For example the smallest graph with automorphism group C_3 has 9 points and 15 lines, see Harary [5, page 170]. However it is easy to find a directed graph with a cyclic automorphism group. For example the automorphism group of the directed graph in Figure 2.7 is isomorphic to

$$C_{S_6}\big((1,2,3)(4,5,6)\big) \cong C_3 \wr S_2.$$

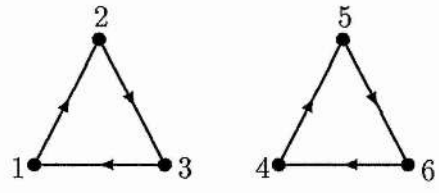


Figure 2.7: A directed graph whose automorphism group is $C_3 \wr S_2$.

Similarly, the automorphism group of the directed graph in Figure 2.8 is isomorphic to

$$C_{S_{12}}\big((1,2,3,4)(5,6,7,8)(9,10,11,12)\big) \cong C_4 \wr S_3.$$

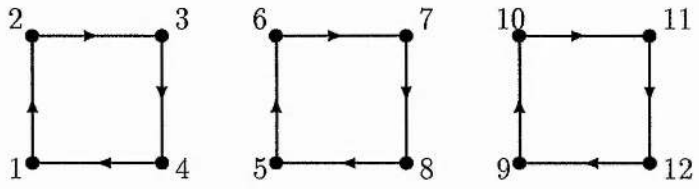


Figure 2.8: A directed graph whose automorphism group is $C_4 \wr S_3$.

In general, if σ is a product of k disjoint m-cycles one can show that the centraliser of σ in S_{mk} is isomorphic to the automorphism group of the graph Γ in Figure 2.9. This is easy to see since an automorphism of Γ can be obtained by performing an arbitrary automorphism on each of the k m-gons, and then following this by any permutation of the m-gons among themselves. (See Hoffmann [6, Chapter VI, Section 4.2] and Wells [20].)

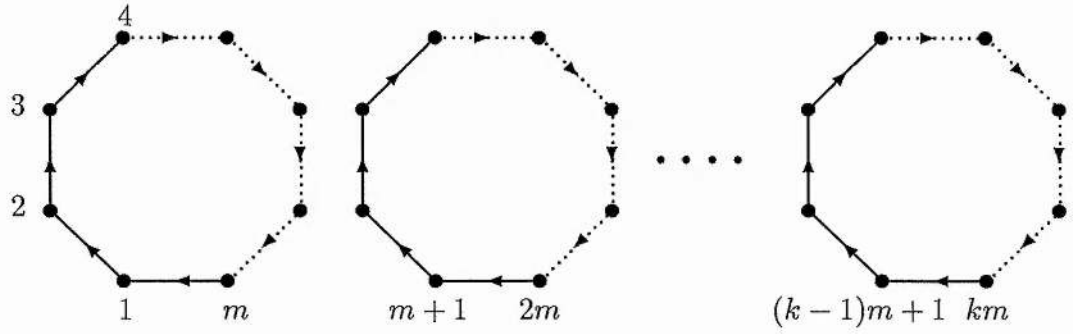


Figure 2.9: A directed graph whose automorphism group is $C_m \wr S_k$.

Remark 2.4.1 In Harary [5, Chapter 14], the "corona" of two graphs G_1 and G_2 (denoted by $G_1 \circ G_2$) is defined to be the graph obtained by taking one copy

of G_1 (which has p_1 points) and p_1 copies of G_2, and then joining the i-th point of G_1 to every point in the i-th copy of G_2. Again in Harary [5] it is shown that

$$\mathrm{Aut}(G_1 \circ G_2) \cong \mathrm{Aut}(G_2) \wr \mathrm{Aut}(G_1)$$

if and only if G_1 or $\overline{G}_2$ has no isolated points (where $\overline{G}_2$ is the complement of G_2). (See also Harary [4].)

As an example, the corona of the complete graphs K_4 and K_2 is shown in Figure 2.10. This has automorphism group $C_2 \wr S_4$ which is the same as the automorphism group of the graph in Figure 2.5.

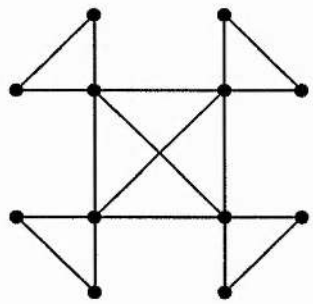


Figure 2.10: A connected graph whose automorphism group is $C_2 \wr S_4$.

In general if σ is not a regular permutation, the centraliser of σ is isomorphic to the automorphism group of a directed graph which is the disjoint union of the graphs corresponding to the regular parts of σ. (See Wells [20] and Hoffmann [6, Chapter VI, Section 4.2].)

Example 2.4.2 Let $\sigma = (1,2)(3,4)(5,6,7)(8,9,10)(11,12,13,14) \in S_{14}$. Then $C_{S_{14}}(\sigma)$ is isomorphic to the automorphism group of the graph in Figure 2.11.

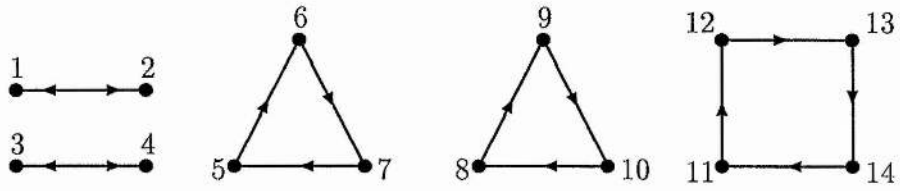


Figure 2.11: A directed graph whose automorphism group is $C_{S_{14}}(\sigma)$.

2.5 Generators and Relations for the Centraliser

In this section we find a presentation for $C_m \wr S_k$. A presentation for the regular wreath product of two groups was given in Johnson [8, 10]. A matrix representation for $C_m \wr S_k$ and a presentation for $C_2 \wr S_k$ are given in Humphreys [7]. We are going to adopt the same notation as Humphreys [7] and we shall extend this presentation to $C_m \wr S_k$.

Let σ be a regular permutation in S_{mk}, say

$$\sigma = (1, 2, \ldots, m)(m+1, m+2, \ldots, 2m) \ldots \big((k-1)m+1, \ldots, km\big).$$

We let β_i, $1 \leqslant i \leqslant k-1$, be the permutations which swap blocks i and $i+1$. As permutations in S_{mk}, these correspond to:

$$\begin{aligned}
\beta_1 &= (1, m+1)(2, m+2) \ldots (m, 2m), \\
\beta_2 &= (m+1, 2m+1)(m+2, 2m+2) \ldots (2m, 3m), \\
&\vdots \\
\beta_{k-1} &= \big((k-2)m+1, (k-1)m+1\big) \big) \ldots (km-m, km).
\end{aligned}$$

Since β_i's act on blocks and S_k can be generated by $(1,2), (2,3), \ldots, (k-1, k)$ it is easy to see that $\langle \beta_1, \beta_2, \ldots, \beta_{k-1} \rangle$ is isomorphic to S_k which acts on blocks. Let β_k be the last block, that is

$$\beta_k = \big((k-1)m+1, \ldots, km\big)$$

which generates the k-th copy of C_m. As we explained in Section 2.3, to generate $C_m \wr S_k$ we need a generator for one copy of C_m and the group S_k. Therefore $\langle \beta_1, \ldots, \beta_k \rangle$ is isomorphic to $C_m \wr S_k$.

Theorem 2.5.1 $C_m \wr S_k$ has the following presentation:

$$\begin{aligned}
C_m \wr S_k = \langle\, b_1, b_2, \ldots, b_k \;\; | \\
{b_i}^2 &= 1 \quad \text{for } 1 \leqslant i \leqslant k-1, && (2.1)\\
(b_i b_{i+1})^3 &= 1 \quad \text{for } 1 \leqslant i \leqslant k-2, && (2.2)\\
[b_i, b_j] &= 1 \quad \text{for } 1 \leqslant i, j \leqslant k-1, |i-j| > 1, && (2.3)\\
{b_k}^m &= 1, && (2.4)\\
[b_i, b_k] &= 1 \quad \text{for } 1 \leqslant i \leqslant k-2, && (2.5)\\
[b_k, {b_k}^{b_{k-1}}] &= 1 \quad \rangle. && (2.6)
\end{aligned}$$

Proof:

Let G be the abstract group with generators $b_1, \ldots, b_k$ satisfying the above relations (2.1)–(2.6). We can define a map from G to $C_m \wr S_k$ by mapping these abstract generators to the permutations $\beta_1, \ldots, \beta_k$ defined above.

It is easy to verify that the relators are mapped to the identity and so this is a homomorphism from G to $C_m \wr S_k$. Since generators for $C_m \wr S_k$ are in the image, this map is clearly onto. To complete the proof we show that there are at most $k!m^k$ elements in G and since this is the order of $C_m \wr S_k$ the map will therefore be one-one. To demonstrate this we show that every element of G can be written in a standard form.

Now we define the following:

$$\begin{aligned}
c_k &= b_k,\\
c_{k-1} &= {c_k}^{b_{k-1}},\\
c_{k-2} &= {c_{k-1}}^{b_{k-2}},\\
&\vdots\\
c_2 &= {c_3}^{b_2},\\
c_1 &= {c_2}^{b_1}.
\end{aligned}$$

Notice that c_k has order m and since the other c_i's are conjugates of c_k they also have order m. Note that c_i maps on to the generator of the i-th copy of C_m in $C_m \wr S_k$. Now we are going to show that c_i's commute. Notice that

$$c_i = b_i b_{i+1} \dots b_{k-1} b_k b_{k-1} \dots b_{i+1} b_i.$$

We have

$$c_k b_{k-1} = b_k b_{k-1} = b_{k-1} b_{k-1} b_k b_{k-1} = b_{k-1} c_{k-1}. \tag{2.7}$$

We have

$$b_i c_i = b_i b_i b_{i+1} \dots b_k \dots b_{i+1} b_i = c_{i+1} b_i, \quad \text{for } 1 \leqslant i \leqslant k-1. \tag{2.8}$$

Similarly

$$c_i b_i = b_i c_{i+1}, \quad \text{for } 1 \leqslant i \leqslant k-1. \tag{2.9}$$

Let $1 \leqslant i \leqslant k-1$. Then

$$\begin{aligned} c_k c_i &= b_k b_i b_{i+1} \dots b_k \dots b_{i+1} b_i \\ &= b_i b_{i+1} \dots b_{k-2} (b_k b_{k-1} b_k b_{k-1}) b_{k-2} \dots b_{i+1} b_i && \text{by (2.5)} \\ &= b_i b_{i+1} \dots b_{k-2} (b_{k-1} b_k b_{k-1} b_k) b_{k-2} \dots b_{i+1} b_i && \text{by (2.6)} \\ &= b_i b_{i+1} \dots b_{k-2} b_{k-1} b_k b_{k-1} b_{k-2} \dots b_{i+1} b_i b_k && \text{by (2.5)} \\ &= c_i c_k. \end{aligned}$$

Therefore

$$c_k c_i = c_i c_k, \quad \text{for } 1 \leqslant i \leqslant k-1. \tag{2.10}$$

Let $1 \leqslant j < i \leqslant k-1$. Then

$$\begin{aligned}
b_i c_j &= b_i b_j b_{j+1} \dots b_k \dots b_{j+1} b_j \\
&= b_j b_{j+1} \dots b_{i-2}(b_i b_{i-1} b_i) b_{i+1} \dots b_k \dots b_{j+1} b_j && \text{by (2.3)} \\
&= b_j b_{j+1} \dots b_{i-2}(b_{i-1} b_i b_{i-1}) b_{i+1} \dots b_k \dots b_{j+1} b_j && \text{by (2.2)} \\
&= b_j b_{j+1} \dots b_k \dots b_{i+1}(b_{i-1} b_i b_{i-1}) b_{i-2} \dots b_j && \text{by (2.3)} \\
&= b_j b_{j+1} \dots b_k \dots b_{i+1}(b_i b_{i-1} b_i) b_{i-2} \dots b_j && \text{by (2.2)} \\
&= b_j b_{j+1} \dots b_k \dots b_{i+1} b_i b_{i-1} b_{i-2} \dots b_j b_i && \text{by (2.3)} \\
&= c_j b_i.
\end{aligned}$$

Therefore

$$b_i c_j = c_j b_i, \quad \text{for } 1 \leqslant j < i \leqslant k-1. \tag{2.11}$$

Let $1 < i+1 < j \leqslant k-1$. Then

$$\begin{aligned}
b_i c_j &= b_i b_j b_{j+1} \dots b_k \dots b_{j+1} b_j \\
&= b_j b_{j+1} \dots b_k \dots b_{j+1} b_j b_i && \text{by (2.3)} \\
&= c_j b_i.
\end{aligned}$$

Therefore

$$b_i c_j = c_j b_i, \quad \text{for } 1 < i+1 < j \leqslant k-1. \tag{2.12}$$

So the formulas we have found so far will allow us to replace $b_i c_j$ (respectively $c_j b_i$) with $b_{i'} c_{j'}$ (respectively $c_{j'} b_{i'}$) for some i', j' with $1 \leqslant i', j' \leqslant k$.

Now let $1 \leqslant j < i \leqslant k$. Now we prove:

$$\begin{aligned}
c_i c_j &= b_i b_{i+1} \dots b_k \dots b_{i+1} b_i \cdot c_j \\
&= c_j b_i b_{i+1} \dots b_k \dots b_{i+1} b_i && \text{by (2.11) or (2.10) if } i = k \\
&= c_j c_i.
\end{aligned}$$

Now, we are going to prove that every word w in $b_1, \ldots, b_k$ can be written as

$$w = \sigma \cdot {c_1}^{\alpha_1} \cdot \cdots \cdot {c_k}^{\alpha_k} \tag{2.13}$$

where σ is a word in $b_1, \ldots, b_{k-1}$. We define $l(w)$ to be the sum of the number of b_i's in σ and the number of ${c_i}^{\alpha_i}$'s. For example, when $k = 4$, $l(w) = 11$ for the following word

$$w = b_2 b_3 b_2 b_1 b_2 b_3 b_2 {c_1}^2 {c_2}^2 {c_3}^3 c_4.$$

Now it is clear when $l(w) = 1$ then w is in the form (2.13). Now let each word w with $l(w) = N$ be in the form (2.13). Let w_1 be a word with $l(w) = N + 1$. It is clear that

$$w_1 = b_i \cdot w$$

where

$$w = \sigma \cdot {c_1}^{\alpha_1} \cdot \cdots \cdot {c_k}^{\alpha_k}.$$

If $i \neq k$ then we let

$$\sigma_1 = b_i \cdot \sigma$$

so that w is still in the form (2.13). But if $i = k$ then when moving $b_k = c_k$ to the right we use (2.5) until we get $b_k b_{k-1}$. Then we replace it by $b_{k-1} c_{k-1}$, using (2.7), to get c_{k-1} in the middle. Then we deal with c_{k-1}. Using the other equations we get c_j (for some j) at the right end. Since it commutes with other c_i's we get

$$w_1 = \tilde{\sigma} \cdot {c_1}^{\alpha_1} \ldots {c_j}^{\alpha_j + 1} \ldots {c_k}^{\alpha_k}$$

where $\tilde{\sigma}$ is a word in $b_1, \ldots, b_{k-1}$ as required.

It is a standard result that the group generated by $\{ b_1, \ldots, b_{k-1} \}$ with the relations (2.1)–(2.3) is isomorphic to S_k (see Johnson [11, pages 61-64]). Every c_i has order m and so there are at most $k! \cdot m^k$ words of this form.

This completes the proof of the theorem. □

Remark 2.5.2 When $m = 2$ one can write the above relations more economically. In this case we get the relations below:

$$\begin{aligned}
{b_1}^2 = {b_2}^2 = \cdots = {b_k}^2 &= 1; \\
(b_i b_{i+1})^3 &= 1 \quad \text{for } 1 \leqslant i \leqslant k-2; \\
(b_{k-1} b_k)^4 &= 1; \\
(b_i b_j)^2 &= 1 \quad \text{for } 1 \leqslant i, j \leqslant k-1, |i-j| > 1; \text{ and} \\
(b_i b_k)^2 &= 1 \quad \text{for } 1 \leqslant i \leqslant k-2.
\end{aligned}$$

These are the relations given in Humphreys [7, page 172].

Example 2.5.3 Let $\sigma = (1,2,3)(4,5,6)(7,8,9)(10,11,12) \in S_{12}$. Then the centraliser of σ in S_{12} has the following presentation.

$$\begin{aligned}
C_{S_{12}}(\sigma) = \langle \; & b_1, b_2, b_3, b_4 \mid \\
& {b_1}^2 = {b_2}^2 = {b_3}^2 = 1, \\
& (b_1 b_2)^3 = (b_2 b_3)^3 = 1, \\
& [b_1, b_3] = 1, \\
& {b_4}^3 = 1, \\
& [b_1, b_4] = [b_2, b_4] = 1, \\
& [b_4, {b_4}^{b_3}] = 1 \quad \rangle.
\end{aligned}$$

2.6 The Centre of $C_{S_n}(\sigma)$

First of all, we find the centre of $C_{S_{mk}}(\sigma) = C_m \wr S_k$ for a regular permutation σ. Then we generalise our result to a general σ. It is a standard result that if G is an abelian group and $H \leqslant S_k$ is a transitive group then the centre of $G \wr H$ is the diagonal copy $\{(g, g, \ldots, g) \mid g \in G\}$. In our case this group is just $\langle\sigma\rangle$. Now we prove it using our notation.

Theorem 2.6.1 Let σ be a regular permutation in S_{mk} which is a product of k disjoint m-cycles with $m > 1$. Let $G = C_{S_{mk}}(\sigma)$. Then we have:

$$Z\big(C_{S_{mk}}(\sigma)\big) = \langle\sigma\rangle.$$

Proof:

Let σ be the permutation:

$$\sigma = (1, 2, \ldots, m)(m+1, m+2, \ldots, 2m)\ldots\big((k-1)m+1, \ldots, km\big).$$

First we show that $\langle\sigma\rangle \subseteq Z(G)$. Let $\tau \in G$ so that $\tau^{-1}\sigma\tau = \sigma$. Now we have:

$$\tau\sigma^r = \tau(\tau^{-1}\sigma\tau)^r = \tau(\tau^{-1}\sigma^r\tau) = \sigma^r\tau \Longrightarrow \langle\sigma\rangle \subseteq Z(G).$$

Now we show that an element in the centre of G must be a power of σ. From Section 2.3 we know that G is generated by $\{\alpha, \beta, \gamma\}$ where

$$\begin{aligned}
\alpha &= (1, 2, \ldots, m),\\
\beta &= (1, m+1)(2, m+2)\ldots(m, 2m),\\
\gamma &= \big(1, m+1, \ldots, (k-1)m+1\big)\big)\ldots(m, 2m, \ldots, km).
\end{aligned}$$

Now, $z \in Z(G)$ if and only if $z^{-1}\alpha z = \alpha$, $z^{-1}\beta z = \beta$ and $z^{-1}\gamma z = \gamma$. From $z^{-1}\alpha z = \alpha$ we must have $1z = r + 1$ for some r with $0 \leqslant r \leqslant m - 1$. For this value of $1z$ we are going to show that $z = \sigma^r$. We have the following picture (where $[r + i]$ stands for "$(r + i)$ mod m"):

$$\left\{\begin{array}{ccccccc} \alpha = (& 1, & 2, & 3, & \dots & ,m &) \\ & \downarrow & \downarrow & \downarrow & & \downarrow & \\ \alpha = (& r+1, & [r+2], & [r+3], & \dots & ,[r+m] &) \end{array}\right\}$$

From the picture above we have

$$iz \equiv (r+i) \pmod{m}, \quad \text{for} \quad 1 \leqslant i \leqslant m.$$

In order to show that $z = \sigma^r$ we need to show

$$(im+1)z = (im+1) + r, \quad \text{for} \quad 0 \leqslant i \leqslant (k-1).$$

Now, from $z^{-1}\gamma z = \gamma$ we have the following picture:

$$\left\{\begin{array}{ccccccc} \gamma = (& 1, & m+1, & 2m+1, & \dots & ,(k-1)m+1 &)\dots \\ & \downarrow & \downarrow & \downarrow & & \downarrow & \\ \gamma = (& r+1, & m+r+1, & 2m+r+1, & \dots & ,(k-1)m+r+1 &)\dots \end{array}\right\}$$

which gives us that $z = \sigma^r$. □

Remark 2.6.2 In general the centre of the centraliser of an element σ will be larger that $\langle\sigma\rangle$. The easiest example is to take $\sigma = id$ in any group G. Then the whole of G is the centraliser but $Z(G)$ may be much larger then $\{id\}$.

Remark 2.6.3 In the proof of the above result, we only needed the fact that $\langle\gamma\rangle$ acted transitively on the blocks. Consequently the result

$$Z(C_m \wr H) = \langle\sigma\rangle$$

holds for any subgroup H of S_k which acts transitively. In particular, this result holds if H is the alternating group A_k, the cyclic subgroup of S_k generated by a k-cycle or the dihedral group D_k.

However, note that in general, if $H \neq S_k$, the centraliser of σ in H is not the wreath product $C_m \wr H$.

Now we illustrate this result by the following example.

Example 2.6.4 Let $\sigma = (1,2,3,4,5)(6,7,8,9,10)(11,12,13,14,15) \in S_{15}$, and let $z \in Z\big(C_{S_{15}}(\sigma)\big)$. A set of generators for $C_{S_{15}}(\sigma)$ is the following:
$\{\alpha = (1,2,3,4,5), \beta = (1,6)(2,7)(3,8)(4,9)(5,10),$
$\gamma = (1,6,11)(2,7,12)(3,8,13)(4,9,14)(5,10,15)\}$.

From $z^{-1}\alpha z = \alpha$ we must have $1z \in \{1,2,3,4,5\}$. Let's suppose $1z = 4$, then we will show that $z = \sigma^3$. We have the following picture:

$$\left.\begin{array}{rl} \alpha = & (1,2,3,4,5) \\ & \downarrow \\ \alpha = & (4,5,1,2,3) \end{array}\right\} \Longrightarrow 1z = 4, 2z = 5, 3z = 1, 4z = 2, 5z = 3.$$

Now, from $z^{-1}\gamma z = \gamma$ we get the following picture, where we replace the values we obtained from the previous picture. We see that there is only one way to fill the bottom row.

$$\left\{\begin{array}{rccccc} \gamma = & (1,6,11) & (2,7,12) & (3,8,13) & (4,9,14) & (5,10,15) \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \gamma = & (4,9,14) & (5,10,15) & (1,6,11) & (2,7,12) & (3,8,13) \end{array}\right\}$$

Since we have all the symbols in the previous picture we must have

$$z = (1,4,2,5,3)(6,9,7,10,8)(11,14,12,15,13) = \sigma^3. \qquad \square$$

Now, we generalise our result to an arbitrary permutation σ.

Theorem 2.6.5 Let $\sigma \in S_n$ be a product of the regular permutations as in Theorem 2.2.1. Then

$$Z\big(C_{S_n}(\sigma)\big) \cong \langle \sigma_{m_1}, \sigma_{m_2}, \ldots, \sigma_{m_r} \rangle \times Z\big(S(\Omega_1)\big).$$

Proof:

The centre of a direct product is the direct product of centres and so the result follows from Theorem 2.2.1. □

Remark 2.6.6 The centre of $S(\Omega_1)$ is non-trivial if and only if $|\Omega_1| = 2$. It follows that:

Corollary 2.6.7 If m_i's are pairwise coprime and the number of points σ leaves fixed is not 2 then we have:

$$Z\big(C_{S_n}(\sigma)\big) = \langle\sigma\rangle.$$ □

Example 2.6.8 Let $\sigma = (1,2,3)(4,5)(6,7,8)(9,10,11,12) \in S_{12}$. Then:

$$\begin{aligned} Z\big(C_{S_{12}}(\sigma)\big) &= \big\langle (4,5), (1,2,3)(6,7,8), (9,10,11,12) \big\rangle \\ &\cong C_2 \times C_3 \times C_4. \end{aligned}$$

In this case $\langle\sigma\rangle$ has index 2 in this group.

Example 2.6.9 Let $\sigma = (1,2)(3,4,5,6,7)(8,9,10,11,12) \in S_{14}$. Then:

$$\begin{aligned} Z\big(C_{S_{14}}(\sigma)\big) &= \big\langle (1,2), (3,4,5,6,7)(8,9,10,11,12), (13,14) \big\rangle \\ &\cong C_2 \times C_5 \times S_2 \\ &\cong \langle\sigma\rangle \times S_2. \qquad \text{(since 2 and 5 are coprime).} \end{aligned}$$

Example 2.6.10 Let
$\sigma = (1,2)(3,4,5)(6,7,8,9,10)(11,12,13,14,15,16,17) \in S_n$, then we have:

$$Z\big(C_{S_n}(\sigma)\big) = \begin{cases} \langle\sigma\rangle, & \text{if } n = 17, 18, 20, 21, \ldots \\ \langle\sigma\rangle \times S_2, & \text{if } n = 19. \end{cases}$$

Chapter 3

Normalisers of Cyclic Subgroups in S_n

3.1 Introduction

In this chapter we examine the structure of the normaliser in S_n of a cyclic subgroup generated (say) by $\sigma \in S_n$. We first investigate the regular case and show that it can be written as a semidirect product of the centraliser of σ by another subgroup which is isomorphic to $\mathrm{Aut}(C_m)$. In the general case we show that the normaliser of $\langle\sigma\rangle$ is a normal subgroup of the direct product of the normalisers of subgroups generated by the regular parts. We find the index and the condition for these two groups to be isomorphic. We show that the normaliser is a direct product in some cases and we give a presentation of the normaliser in the regular case.

The normaliser of a subgroup H in G, denoted by $N_G(H)$, is defined as:

$$N_G(H) = \{\, x \in G \mid x^{-1}Hx = H \,\}.$$

Note that $N_G(H)$ always contains H, and is a subgroup of G. We have the

following standard proposition.

Proposition 3.1.1 Let H be a subgroup of the group G. Then $C_G(H)$ is a normal subgroup of $N_G(H)$ and $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Proof:

For each x in $N_G(H)$, define a map $\vartheta_x : H \to H$ by $h\vartheta_x = x^{-1}hx$. The map ϑ_x is clearly a homomorphism and has inverse $\vartheta_{x^{-1}}$ and is thus an automorphism.

The map $x \longmapsto \vartheta_x$ is a homomorphism since

$$h\vartheta_x\vartheta_y = (x^{-1}hx)\vartheta_y = y^{-1}x^{-1}hxy = (xy)^{-1}h(xy) = h\vartheta_{xy}.$$

The kernel of this map is easily seen to be $C_G(H)$, and so the result follows by the First Isomorphism Theorem. □

Let σ be an element of S_n. We first write σ as a product of disjoint cycles and we define σ_{m_i}'s and Ω_{m_i}'s as in Theorem 2.2.1.

Proposition 3.1.2 Let $\sigma \in S_n$. Then

$$N_{S_n}(\langle\sigma\rangle) = \{\, h \in S_n \mid h^{-1}\sigma h = \sigma^t \text{ for some } t \text{ with } (t, |\sigma|) = 1, 1 \leqslant t < |\sigma| \,\}.$$

Proof:

If $h \in N_{S_n}(\langle\sigma\rangle)$, we have

$$h^{-1}\langle\sigma\rangle h = \langle h^{-1}\sigma h\rangle$$

and this is isomorphic to $\langle\sigma\rangle$ if and only if $h^{-1}\sigma h = \sigma^t$ with σ^t a generator of the cyclic group $\langle\sigma\rangle$. This happens if and only if t and the order of σ are coprime. Hence

$$N_{S_n}(\langle\sigma\rangle) = \{\, h \in S_n \mid h^{-1}\sigma h = \sigma^t, (t, |\sigma|) = 1, 1 \leqslant t < |\sigma| \,\}.$$ □

Example 3.1.3 Let $\sigma = (1,2,3)(4,5)(6,7)(8,9,10,11) \in S_{11}$.
$|\sigma| = \text{lcm}(2,3,4) = 12$. So,

$$N_{S_{11}}(\langle\sigma\rangle) = \{\, h \in S_{11} \mid h^{-1}\sigma h = \sigma^t, t = 1,5,7 \text{ or } 11 \,\}.$$

We will see later that $N_{S_{11}}(\langle\sigma\rangle)$ is a group of order 384.

3.2 Normalisers of Subgroups Generated by Regular Permutations in S_n

As before, we first investigate the case of a regular permutation. Let σ be a product of k disjoint m-cycles, say

$$\sigma = (1, 2, \ldots, m)(m+1, m+2, \ldots, 2m) \ldots ((k-1)m+1, \ldots, km).$$

Now by the previous proposition

$$N_{S_{mk}}(\langle\sigma\rangle) = \{\, h \in S_{mk} \mid h^{-1}\sigma h = \sigma^t \text{ with } (t, m) = 1 \,\}.$$

Notice that the elements for which $t = 1$ lie in the centraliser of σ in S_{mk}.

Example 3.2.1 Let $\sigma = (1, 2, 3, 4)(5, 6, 7, 8) \in S_8$. Then $m = 4$ so that $t = 1$ or $t = 3$. Therefore

$$\begin{aligned} N_{S_8}(\langle\sigma\rangle) &= \{\, h \in S_8 \mid h^{-1}\sigma h = \sigma \text{ or } h^{-1}\sigma h = \sigma^3 \,\} \\ &= C_{S_8}(\sigma) \cup \{\, h \in S_8 \mid h^{-1}\sigma h = \sigma^3 \,\} \qquad \text{(disjoint union)}. \end{aligned}$$

Now the order of $C_{S_8}(\sigma)$ and the order of $\{\, h \in S_8 \mid h^{-1}\sigma h = \sigma^3 \,\}$ are $2!4^2 = 32$ and order of the normaliser is 64.

In general, if σ is a product of k disjoint m-cycles and $\phi(m)$ is the number of positive integers coprime to m and less than m then we will prove that

$$\left|N_{S_{mk}}(\langle\sigma\rangle)\right| = \phi(m) \cdot k! \cdot m^k.$$

Note that $k! \cdot m^k$ is the size of $C_{S_{mk}}(\sigma)$ which is $C_m \wr S_k$. So our result will show that $C_{S_{mk}}(\sigma)$ is a normal subgroup of $N_{S_{mk}}(\langle\sigma\rangle)$ with index $\phi(m)$.

We now examine the structure of the group $N_{S_{mk}}(\langle\sigma\rangle)$ in more detail.

Let σ be a product of k disjoint m-cycles. Then every element of $C_{S_{mk}}(\sigma)$ can be uniquely written as

$$[h'; c_1, \ldots, c_k] \quad \text{where } c_i \in C_m \text{ and } h' \in S_k.$$

The multiplication is defined, for $f', h' \in S_k; c_i, d_i \in C_m$, as follows:

$$[h'; c_1, \ldots, c_k] \cdot [f'; d_1, \ldots, d_k] = [h'f'; c_{1f^{-1}} \cdot d_1, \ldots, c'_{kf^{-1}} \cdot d_k]. \tag{3.1}$$

Lemma 3.2.2 There is an action of $\mathrm{Aut}(C_m)$ on $C_{S_{mk}}(\sigma)$ when we define:

$$[h'; c_1, \ldots, c_k]^\theta = [h'; c_1\theta, \ldots, c_k\theta]; \tag{3.2}$$

for $h' \in S_k, c_i \in C_m, \theta \in \mathrm{Aut}(C_m)$.

Proof:

Let $h', f' \in S_k$; $c_i, d_i \in C_m$ and $\theta, \alpha \in \mathrm{Aut}(C_m)$. We are going to show that the conditions of Definition 1.3.3 are satisfied.

i) $$\begin{aligned}\left[[h'; c_1, \ldots, c_k]^\theta\right]^\alpha &= [h'; c_1\theta, \ldots, c_k\theta]^\alpha \\ &= [h'; c_1\theta\alpha, \ldots, c_k\theta\alpha] \\ &= [h'; c_1, \ldots, c_k]^{\theta\alpha};\end{aligned}$$

ii) $[h'; c_1, \ldots, c_k]^1 = [h'; c_1, \ldots, c_k]$;

iii) $$\begin{aligned}\Big[[h'; c_1, \ldots, c_k] \cdot [f'; d_1, \ldots, d_k]\Big]^\theta &= [h'f'; c_{1f^{-1}} \cdot d_1, \ldots, c_{kf^{-1}} \cdot d_k]^\theta \\ &= [h'f'; c_{1f^{-1}}\theta \cdot d_1\theta, \ldots, c_{kf^{-1}}\theta \cdot d_k\theta] \\ &= [h'; c_1\theta, \ldots, c_k\theta][f'; d_1\theta, \ldots, d_k\theta] \\ &= [h'; c_1, \ldots, c_k]^\theta \cdot [f'; d_1, \ldots, d_k]^\theta. \qquad \square\end{aligned}$$

Remark 3.2.3 The automorphism group of C_m is the group U_m of units in $\mathbb{Z}_m$ and consists of all elements of $\mathbb{Z}_m$ coprime to m. Its order is the Euler function $\phi(m)$. It is cyclic if and only if m is $2, 4, p^k, 2p^k$ for p an odd prime and k any integer.

Proposition 3.2.4 Let $\sigma \in S_n$ (not necessarily regular) with $|\sigma| = m$ and let $h \in N_{S_n}(\langle\sigma\rangle)$ conjugate σ into σ^r with $(r, m) = 1$. Let $\bar{r}$ represent the inverse of r in $U(\mathbb{Z}_m)$, the group of units in $\mathbb{Z}_m$, in other words $r\bar{r} \equiv 1 \pmod{m}$. Then h^{-1} conjugates σ into $\sigma^{\bar{r}}$.

Proof:

$$\begin{aligned} h^{-1}\sigma h = \sigma^r &\Rightarrow h\sigma^r h^{-1} = \sigma \\ &\Rightarrow (h\sigma^r h^{-1})^{\bar{r}} = \sigma^{\bar{r}} \\ &\Rightarrow h\sigma h^{-1} = \sigma^{\bar{r}}. \end{aligned}$$ □

Theorem 3.2.5 Let σ be a product of k disjoint m-cycles, say

$$\sigma = (1, 2, \ldots, m)(m+1, m+2, \ldots, 2m)\ldots((k-1)m+1, \ldots, km).$$

Let ϕ denote the action of $\mathrm{Aut}(C_m)$ on $C_{S_{mk}}(\sigma)$ defined above. Then $N_{S_{mk}}(\langle\sigma\rangle)$ is the semidirect product $\mathrm{Aut}(C_m) \,{}_{\phi}\!\times C_{S_{mk}}(\sigma)$.

Proof:

Let $C = C_{S_{mk}}(\sigma)$ and $N = N_{S_{mk}}(\langle\sigma\rangle)$. We now define a subgroup of N which we will show is isomorphic to $\mathrm{Aut}(C_m)$. Let F be the set of symbols written first in each of the above disjoint m-cycles, i.e.

$$F = \{\, 1 + mi \mid 0 \leqslant i \leqslant k-1 \,\}$$

For each $t \in \mathbb{Z}_m$ which is coprime to m, we choose an element $h_t \in N_{S_{mk}}(\langle\sigma\rangle)$ in the following way. We choose h_t to fix the symbols in F. We then choose h_t so that it conjugates σ into σ^t. Since it then maps each m-cycle τ to τ^t, it is defined on each element of τ and hence on the whole of the set of symbols. Since σ and σ^t have the same cycle shape and F contains a symbol from each block it is always possible to choose h_t with the required properties. (See example below.)

We show that $\{\, h_t \mid t \text{ a unit in } \mathbb{Z}_m \,\}$ is a subgroup of $N_{S_{mk}}(\langle\sigma\rangle)$ which is isomorphic to the group U_m. We need only show that the map $t \longmapsto h_t$ from

U_m to $N_{S_{mk}}(\langle\sigma\rangle)$ is a homomorphism since it is clearly one-one onto its image. To show this let $t_1, t_2 \in U_m$. First of all, let x be a symbol in the first m-cycle. The proof for other cycles can be done similarly. We notice that the symbol x is mapped to

$$1 + (x-1)t_1 \pmod{m}$$

under h_{t_1} (except that the number 0 is replaced by m). So that under $h_{t_1}h_{t_2}$ the symbol x is mapped to

$$1 + \big(1 + (x-1)t_1 - 1\big)t_2 \equiv 1 + (x-1)t_1t_2 \pmod{m}.$$

Therefore

$$h_{t_1}h_{t_2} = h_{t_1t_2},$$

and we have a homomorphism. From now on we call this set U_m, so

$$U_m = \{\, h_t \mid (t,m) = 1 \,\}.$$

Next we show that $U_m \cap C = 1_N$. Let $u \in U_m$. Since u fixes F and the only element of C which fixes F is (id), it follows that $U_m \cap C = \{\, id \,\}$.

Next we show that $U_mC = N$. Let $\nu \in N$, so that $\nu^{-1}\sigma\nu = \sigma^t$ for some t with $(t,m) = 1$. We will show that ν can be written as a product of elements from U_m and C. Let $h_t \in U_m$ with ${h_t}^{-1}\sigma h_t = \sigma^t$. (i.e. $1h_t = 1$, $(m+1)h_t = m+1, \ldots$). Now, let $c_t = {h_t}^{-1}\nu$. Then

$${c_t}^{-1}\sigma c_t = \nu^{-1}u_t\sigma {u_t}^{-1}\nu = \nu^{-1}\sigma^{\bar{t}}\nu = \sigma^{\bar{t}t} = \sigma,$$

so $c_t \in C$ and $\nu = h_tc_t \in U_mC$. This completes this proof that $U_mC = N$.

Finally, in order to show that the action corresponds to ϕ, we show that the conjugating an element of C by an element of U_m in N corresponds to ϕ (see Theorem 1.3.8). Let $c \in C$, then c can be represented as

$$[h'; c_1, \ldots, c_k] \quad \text{where } h' \in S_k \text{ and } c_i \in C_m.$$

Let $\phi \in \mathrm{Aut}(C_m)$ represent the automorphism $c \mapsto c^t$ with $(t,m) = 1$ and $c \in C_m$. Let $u \in U_m$ be the element h_t defined above, so that $u^{-1}\sigma u = \sigma^t$. Let $h, \alpha_1, \ldots, \alpha_k$ be the permutations in S_{mk} which correspond to $h', c_1, \ldots, c_k$ respectively (as explained in Section 1.5). Then in N we have:

$$u^{-1}cu = u^{-1}hu \cdot u^{-1}\alpha_1 u \cdot \ldots \cdot u^{-1}\alpha_k u.$$

We know that if $u^{-1}\sigma u = \sigma^t$ then $u^{-1}\alpha_i u = {\alpha_i}^t$ and so $c_i\phi = {c_i}^t$. Now, all we need to show is $u^{-1}hu = h$ or, equivalently, $h^{-1}uh = u$. In order to do so we need to show that $h^{-1}uh$ conjugates σ into σ^t and that $h^{-1}uh$ fixes F. Note that, if a is one of the symbols in F then so is $ah^{-1} = b$, and that u fixes F. Now

$$\begin{aligned}(h^{-1}uh)^{-1}\sigma(h^{-1}uh) &= h^{-1}u^{-1}h\sigma h^{-1}uh \\ &= h^{-1}u^{-1}\sigma uh \\ &= h^{-1}\sigma^t h = (h^{-1}\sigma h)^t \\ &= \sigma^t.\end{aligned}$$

Also

$$a(h^{-1}uh) = b(uh) = bh = a.$$

So, $h^{-1}uh = u$ or $u^{-1}hu = h$. Hence the result:

$$N = U_m \,{}_\phi\!\times C \cong \mathrm{Aut}(C_m) \,{}_\phi\!\times C_{S_{mk}}(\sigma). \qquad \square$$

Example 3.2.6 Suppose $\sigma = (1,2,3,4,5)(6,7,8,9,10) \in S_{10}$, so that $m = 5, k = 2$. Then units in $\mathbb{Z}_5$ are $\{1,2,3,4\}$ and we define (say) h_3 by the diagram below.

$$\begin{array}{rcll} \sigma & = & (1,2,3,4,5) & (6,7,8,9,10) \\ & & \downarrow & \downarrow \\ \sigma^3 & = & (1,4,2,5,3) & (6,9,7,10,8) \end{array}$$

so that

$$h_3 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,\;9\,10 \\ 1\,4\,2\,5\,3\,6\,9\,7\,10\;\;8 \end{pmatrix} = (2,4,5,3)(7,9,10,8).$$

3.3 Generators and Relations for the Normaliser

In this section we find a presentation for the normaliser of $\langle\sigma\rangle$ in S_{mk} when σ is a regular permutation which is a product of k disjoint m-cycles. By Theorem 3.2.5 $N = N_{S_{mk}}(\langle\sigma\rangle)$ is a semidirect product of $C = C_{S_{mk}}(\sigma)$ by U_m where U_m is the automorphism group of the cyclic group C_m. The structure of the abelian group U_m depends on number theoretic properties of m. For instance, if m has a primitive root (as outlined in Remark 3.2.3), then U_m is cyclic. In this case N is a semidirect product of the centraliser C by a cyclic group and we will give the presentation for such a semidirect product. A presentation for semidirect products is given in Johnson [11, Chapter 10]. In a presentation of a semidirect product one has to specify the action of one group on the other together with the presentations of both groups.

Assume that U_m is cyclic, say generated by the primitive root r. We adopt the notation used above for the presentation of the centraliser. Assume the centraliser is generated by $\{b_1, \ldots, b_k\}$ with the relations given in Theorem 2.5.1. The element r corresponds to the element h_r introduced in the proof of Theorem 3.2.5 which conjugates σ into σ^r. This element acts trivially on the subgroup $\langle b_1, \ldots, b_{k-1}\rangle$ which is isomorphic to S_k. We introduce a new generator u which will map to this element h_r and which thus satisfies the relations

$$u^{\phi(m)} = 1 \quad \text{and} \quad [b_i, u] = 1 \quad \text{for } 1 \leqslant i \leqslant k-1.$$

Since h_r conjugates σ into σ^r, the action on b_k is given by

$${b_k}^u = {b_k}^r.$$

Following Johnson [11] we deduce the following.

Proposition 3.3.1 The group $N_{S_{mk}}(\langle\sigma\rangle)$ has the following presentation when

U_m is cyclic and generated by the primitive root r.

$$
\begin{aligned}
N_{S_{mk}}(\langle\sigma\rangle) = \langle\ b_1, b_2, \ldots, b_k, u \quad \mid & \\
{b_i}^2 &= 1 \quad \text{for } 1 \leqslant i \leqslant k-1, && (3.3)\\
(b_i b_{i+1})^3 &= 1 \quad \text{for } 1 \leqslant i \leqslant k-2, && (3.4)\\
[b_i, b_j] &= 1 \quad \text{for } 1 \leqslant i, j \leqslant k-1, |i-j| > 1, && (3.5)\\
{b_k}^m &= 1, && (3.6)\\
[b_i, b_k] &= 1 \quad \text{for } 1 \leqslant i \leqslant k-2, && (3.7)\\
[b_k, {b_k}^{b_{k-1}}] &= 1, && (3.8)\\
u^{\phi(m)} &= 1, && (3.9)\\
[b_i, u] &= 1 \quad \text{for } 1 \leqslant i \leqslant k-1, && (3.10)\\
{b_k}^u {b_k}^{-r} &= 1\rangle. && (3.11)
\end{aligned}
$$

□

Example 3.3.2 Let σ be 4 disjoint 5-cycles in S_{20}. Then $U_5 = \{1, 2, 3, 4\}$ which is generated by 2 or 3. Then $N_{S_{20}}(\langle\sigma\rangle)$ has the following presentation.

$$
\begin{aligned}
N_{S_{20}}(\langle\sigma\rangle) = \langle\ & b_1, b_2, b_3, b_4, u \mid \\
& {b_1}^2 = {b_2}^2 = {b_3}^2 = 1, \\
& (b_1 b_2)^3 = (b_2 b_3)^3 = 1, \\
& [b_1, b_3] = 1, \\
& {b_4}^5 = 1, \\
& [b_1, b_4] = [b_2, b_4] = 1, \\
& [b_4, {b_4}^{b_3}] = 1, \\
& u^4 = 1, \\
& [b_1, u] = [b_2, u] = [b_3, u] = 1, \\
& {b_4}^u {b_4}^{-2} = 1 \quad \rangle. \qquad \square
\end{aligned}
$$

When U_m is not cyclic, it is isomorphic to a direct product of cyclic groups. For instance the group of units in $\mathbb{Z}_8$ is

$$U_8 = \{1, 3, 5, 7\} \cong C_2 \times C_2 = \langle 3 \rangle \times \langle 5 \rangle.$$

Now assume that

$$U_m = \langle r_1 \rangle \times \cdots \times \langle r_t \rangle = C_{n_1} \times \cdots \times C_{n_t}$$

where n_i is the order of r_i in U_m. Let u_i be a new generator which represents r_i (and corresponds to h_{r_i}). The cyclic group C_{n_i} has the presentation

$$\langle u_i \mid {u_i}^{n_i} = 1 \rangle.$$

The direct product $C_{n_1} \times \cdots \times C_{n_t}$ is generated by $\{ u_1, \ldots, u_t \}$ and has the following relations (see Johnson [11, page 45]):

$${u_i}^{n_i} = 1, \quad \text{for } 1 \leqslant i \leqslant t, \tag{3.12}$$

$$[u_i, u_j] = 1, \quad \text{for } 1 \leqslant i < j \leqslant t. \tag{3.13}$$

Since h_{r_i} conjugates σ into σ^{r_i}, the action of u_i's on b_i's is given by the following relations:

$$[b_i, u_j] = 1, \quad \text{for } 1 \leqslant i \leqslant k-1, \quad 1 \leqslant j \leqslant t, \tag{3.14}$$

$${b_k}^{u_i} {b_k}^{-r_i} = 1, \quad \text{for } 1 \leqslant i \leqslant t. \tag{3.15}$$

It follows from Johnson [11] that $N_{S_{mk}}(\langle \sigma \rangle)$ is generated by the set

$$\{ b_1, \ldots, b_k, u_1, \ldots, u_t \}$$

with the relations listed in Theorem 2.5.1 and the relations (3.12)-(3.15).

Example 3.3.3 Let σ be three disjoint 8-cycles in S_{24}. Then

$$U_8 = \{ 1, 3, 5, 7 \} = \langle 3 \rangle \times \langle 5 \rangle.$$

Then $N_{S_{24}}(\langle\sigma\rangle)$ has the following presentation.

$$\begin{aligned} N_{S_{24}}(\langle\sigma\rangle) = \langle \; & b_1, b_2, b_3, u_1, u_2 \mid \\ & {b_1}^2 = {b_2}^2 = 1, \\ & (b_1 b_2)^3 = 1, \\ & {b_3}^8 = 1, \\ & [b_1, b_3] = 1 \\ & [b_3, {b_3}^{b_2}] = 1, \\ & {u_1}^2 = {u_2}^2 = 1, \\ & [u_1, u_2] = 1, \\ & [b_1, u_1] = [b_2, u_1] = [b_1, u_2] = [b_2, u_2] = 1, \\ & {b_3}^{u_1} {b_3}^{-3} = {b_3}^{u_2} {b_3}^{-5} = 1 \quad \rangle. \end{aligned}$$

3.4 General Case

Let σ be an element of S_n. Now we prove that $N = N_{S_n}(\langle\sigma\rangle)$ is a semidirect product of its centraliser by a subgroup of N which is isomorphic to $U_{|\sigma|}$.

Theorem 3.4.1 Let σ be an element of S_n with order d. Then the normaliser $N_{S_n}(\langle\sigma\rangle)$ is a semidirect product of $C_{S_n}(\sigma)$ by $\mathrm{Aut}(C_d)$.

Proof:

The proof is similar to the regular case. We first write σ as a product of disjoint cyles and we define $\sigma_{m_i}, \Omega_{m_i}$ and r as in Theorem 2.2.1. Let C and N be the centraliser and normaliser of $\langle\sigma\rangle$ respectively. We note that for every t coprime to d we can find an element in S_n which conjugates σ into σ^t and this elements lies in N. It follows that the map $x \mapsto \vartheta_x$ in the proof of Proposition 3.1.1 is onto and so N/C is isomorphic to $\mathrm{Aut}(C_d)$ and we show that N is a semidirect product of C by $\mathrm{Aut}(C_d)$.

Let U_d be the set of permutations which conjugate σ into σ^t, for some t coprime to d, and fixes the set F (where F is the set of "first symbols" as in the proof of Theorem 3.2.5). Then it easy to show that U_d is a subgroup of N which is isomorphic to $\mathrm{Aut}(C_d)$. It is also easy to show that $U_d \cap C = \{id\}$. We now show that $U_dC = N$. Let $\nu \in N$ conjugate σ into σ^p, then $\nu = \nu_{m_1} \cdot \ldots \cdot \nu_{m_r}$, where ν_{m_i} is an element of the normaliser of $\langle\sigma_{m_i}\rangle$ in $S(\Omega_{m_i})$ and therefore is equal to $u_{m_i}c_{m_i}$ where u_{m_i} conjugates σ_{m_i} into ${\sigma_{m_i}}^p$ and fixes F and $c_{m_i} \in C_{S(\Omega_{m_i})}(\sigma_{m_i})$. Since u_{m_i} and c_{m_j} commute whenever $i \neq j$ we have:

$$\nu = (u_{m_1} \cdot \ldots \cdot u_{m_r}) \cdot (c_{m_1} \cdot \ldots \cdot c_{m_r}).$$

Note that $u = u_{m_1} \cdot \ldots \cdot u_{m_r}$ conjugates σ into σ^p and fixes F, and $c = c_{m_1} \cdot \ldots \cdot c_{m_r}$ is in the centraliser of σ. Therefore $\nu \in U_dC$. □

Note that the centraliser of a general permutation σ was the direct product of the centralisers of the regular permutations σ_{m_i}. In the case of normalisers we do not get such a nice result. However, we prove that the normaliser of the subgroup generated by σ in S_n is a normal subgroup of the direct product of normalisers of the subgroups generated by the σ_{m_i}'s in the $S(\Omega_{m_i})$'s.

Theorem 3.4.2 Let $\sigma \in S_n$. We define σ_{m_i}'s, Ω_{m_i}'s and r as in Theorem 2.2.1. Then

$$N_{S_n}(\langle\sigma\rangle) \trianglelefteq N_{S(\Omega_{m_1})}(\langle\sigma_{m_1}\rangle) \times \ldots \times N_{S(\Omega_{m_r})}(\langle\sigma_{m_r}\rangle). \tag{3.16}$$

Proof:
Let $\nu \in N_{S_n}(\langle\sigma\rangle)$ so that $\nu^{-1}\sigma\nu = \sigma^k$ for some k with $(k, |\sigma|) = 1$. We have

$$\sigma = \sigma_{m_1} \cdot \ldots \cdot \sigma_{m_r}, \text{ so that } \sigma^k = {\sigma_{m_1}}^k \cdot \ldots \cdot {\sigma_{m_r}}^k.$$

Notice that σ_{m_i} and ${\sigma_{m_i}}^k$ have the same cycle structure for every i. In order to find an element $h \in S_n$ which conjugates σ into σ^k we need to find an element in $S(\Omega_{m_1})$ which conjugates σ_{m_1} into ${\sigma_{m_1}}^k$. Let's call this element h_1. Similarly we need to find $h_2, \ldots, h_r$ which conjugate $\sigma_{m_2}, \ldots, \sigma_{m_r}$, respectively, into ${\sigma_{m_2}}^k, \ldots, {\sigma_{m_r}}^k$, respectively; with $h_i \in S(\Omega_{m_i})$. And we multiply them to get $h_1 \cdot h_2 \cdot \ldots \cdot h_r$. This product conjugates σ into σ^k. Therefore the left hand side of (3.16) is a subgroup of the right hand side.

In order to prove the normality we let

$$h_i \in N_i = N_{S(\Omega_{m_i})}(\langle\sigma_{m_i}\rangle) \text{ with } {h_i}^{-1}\sigma_{m_i}h_i = {\sigma_{m_i}}^{\alpha_i}, \text{ where } (\alpha_i, m_i) = 1.$$

Let $\overline{\alpha_i}$ represent the inverse of α_i in U_{m_i} as in Proposition 3.2.4. Let $n \in N$ with $n^{-1}\sigma n = \sigma^t$, and let $h = h_1 \cdot h_2 \cdot \ldots \cdot h_r$. We need to show that $h^{-1}nh \in N$.

$$\begin{aligned}
(h^{-1}nh)^{-1}\sigma(h^{-1}nh) &= h^{-1}n^{-1}h\sigma h^{-1}nh \\
&= h^{-1}n^{-1}h_1 \ldots h_r \sigma {h_r}^{-1} \ldots {h_1}^{-1}nh \\
&= h^{-1}n^{-1}{\sigma_{m_1}}^{\overline{\alpha_1}} \ldots {\sigma_{m_r}}^{\overline{\alpha_r}}nh \\
&= h^{-1}{\sigma_{m_1}}^{\overline{\alpha_1}t} \ldots {\sigma_{m_r}}^{\overline{\alpha_r}t}h \\
&= {\sigma_{m_1}}^{\overline{\alpha_1}t\alpha_1} \ldots {\sigma_{m_r}}^{\overline{\alpha_r}t\alpha_r} \\
&= {\sigma_{m_1}}^{t} \ldots {\sigma_{m_r}}^{t} \\
&= \sigma^t. \qquad \square
\end{aligned}$$

In general, the inclusion of the normal subgroup in the above theorem will be proper.

Example 3.4.3 Let $\sigma = (1,2,3)(4,5,6,7,8,9) \in S_9$ with

$$\sigma_3 = (1,2,3) \text{ and } \sigma_6 = (4,5,6,7,8,9).$$

Now let $\tau_3 \in N_{S_3}\big(\langle\sigma_3\rangle\big)$ and $\tau_6 \in N_{S(\Omega_6)}\big(\langle\sigma_6\rangle\big)$ be such that

$${\tau_3}^{-1}\sigma_3\tau_3 = \sigma_3 \quad \text{and} \quad {\tau_6}^{-1}\sigma_6\tau_6 = {\sigma_6}^5.$$

Now $\tau_3\tau_6 \notin N_{S_9}\big(\langle\sigma\rangle\big)$ because it conjugates σ into $\sigma_3{\sigma_6}^5$ which is not a power of σ. $\square$

Theorem 3.4.4 The index of the normaliser of $\langle\sigma\rangle$ in S_n in the direct product of the normalisers of $\langle\sigma_{m_i}\rangle$'s in $S(\Omega_{m_i})$'s is

$$\frac{\phi(m_1)\ldots\phi(m_r)}{\phi\big(\mathrm{lcm}(m_1,\ldots,m_r)\big)}. \tag{3.17}$$

Proof:

Since the normaliser of $\langle\sigma\rangle$ in S_n is the semidirect product of its centraliser by

a subgroup isomorphic to $U_{|\sigma|}$ (by Theorem 3.4.1) and since the centraliser of σ in S_n is isomorphic to the direct product of centralisers of the regular parts (by Theorem 2.2.1) we have:

$$\begin{aligned}\left|N_{S_n}(\langle\sigma\rangle)\right| &= |C_{S_n}(\sigma)| \cdot |U_{|\sigma|}| \\ &= |C_{m_1} \wr S_{k_1}| \cdot \ldots \cdot |C_{m_r} \wr S_{k_r}| \cdot \phi(|\sigma|) \\ &= k_1! \cdot {m_1}^{k_1} \cdot \ldots \cdot k_r! \cdot {m_r}^{k_r} \cdot \phi\big(\mathrm{lcm}(m_1, \ldots, m_k)\big)\end{aligned}$$

By Theorem 3.2.5 the normaliser of $\langle\sigma_{m_i}\rangle$ in $S(\Omega_{m_i})$ is a semidirect product of its centraliser by a subgroup of order $\phi(m_i)$, so the order of the direct product of the normalisers is:

$$k_1! \cdot {m_1}^{k_1} \cdot \phi(m_1) \cdot \ldots \cdot k_r! \cdot {m_r}^{k_r} \cdot \phi(m_r).$$

Therefore the required index is:

$$\frac{\phi(m_1) \ldots \phi(m_r)}{\phi\big(\mathrm{lcm}(m_1, \ldots, m_r)\big)}.$$

□

Example 3.4.5 By a program written in GAP we find the following:

$N_{S_9}\Big(\big\langle(1,2,3)(4,5,6,7,8,9)\big\rangle\Big)$ has order $36 = 3 \cdot 6 \cdot \phi(6)$,while

$N_{S_3}\Big(\big\langle(1,2,3)\big\rangle\Big) \times N_{S(\Omega_6)}\Big(\big\langle(4,5,6,7,8,9)\big\rangle\Big)$ has order $72 = 3 \cdot \phi(3) \cdot 6 \cdot \phi(6)$. Now,

$$\frac{\phi(3) \cdot \phi(6)}{\phi\big(\mathrm{lcm}(3,6)\big)} = 2$$

which gives us the index. □

It is clear that if the m_i's are pairwise coprime then we have:

$$\phi(m_1) \ldots \phi(m_r) = \phi(m_1 \ldots m_r) = \phi\big(\mathrm{lcm}(m_1, \ldots, m_r)\big).$$

so that the index is one. But the converse is not true, since

$$\phi(2) \cdot \phi(4) \cdot \phi(6) = \phi\big(\mathrm{lcm}(2,4,6)\big).$$

Corollary 3.4.6 The normaliser of $\langle\sigma\rangle$ is isomorphic to the direct product of the normalisers of $\langle\sigma_{m_i}\rangle$'s in $S(\Omega_{m_i})$'s if and only if the odd parts of the m_i's are pairwise coprime and at most one of the m_i's is divisible by 4.

Proof:

Let the odd parts of the m_i's be pairwise coprime and let only one of the m_i's, (say) m_1, have 2^a with $a > 1$ in its prime decomposition. Since $\phi(2) = 1$ and if $\phi(pq) = \phi(p)\phi(q)$ then p, q are coprime, we have

$$\phi\big(\mathrm{lcm}(m_1, \ldots, m_r)\big) = \phi(m_1) \ldots \phi(m_r),$$

so that the index is 1 and these two groups are isomorphic.

Conversely let these two groups be isomorphic. Then the index is 1, i.e.

$$\phi\big(\mathrm{lcm}(m_1, \ldots, m_r)\big) = \phi(m_1) \ldots \phi(m_r). \tag{3.18}$$

We have

$$\mathrm{lcm}(m_1, \ldots, m_r) = \prod_{p_i} {p_i}^{\alpha_i}$$

where the product is taken over all the primes p_i which occur in the prime decompositions of the m_i's and α_i is the highest power of p_i in these prime decompositions. We know that if ${p_1}^{a_1} \ldots {p_t}^{a_t}$ is the prime decomposition of a number m then

$$\phi(m) = \phi({p_1}^{a_1}) \ldots \phi({p_t}^{a_t}).$$

Since $\phi(2) = 1$ and 2 is the only such prime number, it follows that the odd parts of the m_i's must be pairwise coprime, i.e. an odd prime occurs in at most one of the m_i's. Otherwise we would have

$$\phi(m_1) \ldots \phi(m_r) > \phi\big(\mathrm{lcm}(m_1, \ldots, m_r)\big).$$

Note that since $\phi(2) = 1$, if some of the m_i's are divisible by 2, but not by 4 then (3.18) still holds. Now let $n \geqslant 1$ be the number of i for which m_i is divisible by 4, i.e. the number of i for which the m_i has 2^b with $b > 1$ in its prime decomposotion. Let $2^{a_1}, 2^{a_2}, \ldots, 2^{a_n}$ be the numbers occuring in the prime decompositions of the m_i's. Then we have

$$\frac{\phi(m_1)\ldots\phi(m_r)}{\phi(\mathrm{lcm}(m_1,\ldots,m_r))} = \frac{\phi(2^{a_1})\phi(2^{a_2})\ldots\phi(2^{a_n})}{\phi(2^a)}$$

where a is the maximum of the a_i's. Since $a_i > 1$ we have $\phi(2^{a_i}) > 1$ for every i, so the above number is 1 if and only if $n = 1$. So the result follows. □

Example 3.4.7 The following numbers satisfy the condition of the corollary:

$$m_1 = 2 \cdot 3^3 \cdot 5^2,$$
$$m_2 = 2^3 \cdot 7^2,$$
$$m_3 = 2 \cdot 11^3,$$
$$m_4 = 13 \cdot 17.$$

We have shown that $N_{S_n}(\langle\sigma\rangle)$ is a normal subgroup of a direct product and each component in this direct product is the normaliser of a subgroup generated by a permutation which is regular. Now we investigate the centre of $N_{S_n}(\langle\sigma\rangle)$.

3.5 The Centre of $N_{S_n}(\langle\sigma\rangle)$

First we find the centre of $N_{S_{mk}}(\langle\sigma\rangle)$ where σ is a regular permutation which is a product of k disjoint m-cycles. We need the following lemma.

Lemma 3.5.1

$$Z\Big(N_{S_{mk}}(\langle\sigma\rangle)\Big) \lhd \langle\sigma\rangle.$$

Proof:

Let $N = N_{S_{mk}}(\langle\sigma\rangle)$ and $C = C_{S_{mk}}(\sigma)$. By Theorem 2.6.1 we have $Z(C) = \langle\sigma\rangle$. It is enough to show that $Z(N) \subseteq Z(C)$ since every subgroup of a cyclic group (in this case $\langle\sigma\rangle$) is normal. Take $id \neq z \in Z(N)$. Since $\sigma \in N$ we have $z^{-1}\sigma z = \sigma$ which shows that $z \in C$, so $Z(N) \subseteq C$. We also have $zc = cz$ for every $c \in C$ since $C \subseteq N$. So $z \in Z(C)$ showing that $Z(N) \subseteq Z(C)$. □

So, we have proved that in the centre of the normaliser we have only some powers of σ. But which powers?

Theorem 3.5.2 Let σ be a product of k disjoint m-cycles with $m > 1$. Let N be the normaliser of $\langle\sigma\rangle$ in S_{mk}. Then if m is odd, the centre of N is trivial; if m is even the centre of N has order 2 and is generated by $\sigma^{\frac{m}{2}}$.

Proof:

Take $\nu \in N$. We have

$$\nu^{-1}\sigma\nu = \sigma^p, \quad \text{for some } p \text{ with } (p, m) = 1.$$

Take $id \neq z \in Z(N)$. We know that $z = \sigma^t$ for some t with $1 \leqslant t \leqslant m-1$. We must have

$$\begin{aligned}
\nu^{-1}z\nu = z &\Rightarrow \nu^{-1}\sigma^t\nu = \sigma^t \\
&\Rightarrow (\nu^{-1}\sigma\nu)^t = \sigma^t \\
&\Rightarrow \sigma^{pt} = \sigma^t \\
&\Rightarrow pt \equiv t \pmod{m} \\
&\Rightarrow (p-1)t \equiv 0 \pmod{m}.
\end{aligned}$$

Looking at the odd and even cases separately:

If m is odd then $(2, m) = 1$. So there exists $\nu \in N$ with $\nu^{-1}\sigma\nu = \sigma^2$ and we can take $p = 2$. For $p = 2$ we must have

$$(p-1)t \equiv 0 \pmod{m} \Rightarrow t \equiv 0 \pmod{m}.$$

This has a solution only for $t = 0$ since $0 \leqslant t \leqslant m-1$. Hence $Z(N) = \{id\}$.

If m is even then note that $t = m/2$ is a solution since p must be odd. Now we have $(m-1, m) = 1$. So, for $p = m-1$, we must have

$$\begin{aligned}
(p-1)t \equiv 0 \pmod{m} &\text{ for every } 0 \leqslant t \leqslant m-1 \\
&\Rightarrow (m-2)t \equiv 0 \pmod{m} \\
&\Rightarrow mt - 2t \equiv 0 \pmod{m} \\
&\Rightarrow 2t \equiv 0 \pmod{m} \\
&\Rightarrow t = 0 \quad \text{or} \quad t = m/2.
\end{aligned}$$

Therefore, $Z(N) = \langle \sigma^{\frac{m}{2}} \rangle$ if m is even. □

Example 3.5.3

$$Z\Big(N_{S_6}\big(\langle(1,2,3)(4,5,6)\rangle\big)\Big) = \{id\}.$$

$$Z\Big(N_{S_{12}}\big(\langle(1,2,3,4)(5,6,7,8)(9,10,11,12)\rangle\big)\Big) = \big\langle(1,3)(2,4)\ldots(10,12)\big\rangle.$$

Now, we generalise our result about the centre of the normaliser.

Given $\sigma \in S_n$, we write σ as a product of disjoint cycles and define the σ_{m_i}'s, Ω_{m_i}'s and r as in Theorem 2.2.1. Then we have the following theorem.

Theorem 3.5.4

$$Z\big(N_{S_n}(\langle\sigma\rangle)\big) = \prod_{m_i \text{ even}} \langle {\sigma_{m_i}}^{\frac{m_i}{2}} \rangle \times Z\big(S(\Omega_1)\big).$$

Proof:

Let $N = N_{S_n}\big(\langle\sigma\rangle\big)$. Take $z \in Z(N)$. Since $\sigma \in N$ and $z^{-1}\sigma z = \sigma$ we have $z \in C_{S_n}(\sigma)$. Moreover $z \in Z\big(C_{S_n}(\sigma)\big)$. By Theorem 2.6.5, $Z\big(C_{S_n}(\sigma)\big)$ is the direct product of subgroups generated by σ_{m_i}'s (except for σ_1 in the case $|\Omega_1| = 2$). Now since $z^{-1}\sigma z = \sigma$ we have

$$z = z_{m_1} \dots z_{m_r} \cdot z_1 \quad \text{with} \quad {z_{m_i}}^{-1}\sigma_{m_i} z_{m_i} = \sigma_{m_i} \quad \text{and } z_1 \in S(\Omega_1).$$

So by Lemma 3.5.1 we deduce that z_{m_i} is a power of σ_{m_i}, say ${\sigma_{m_i}}^{t_i}$. Let $\nu \in N$. Then $\nu^{-1}\sigma\nu = \sigma^p$ for some p with $(p, |\sigma|) = 1$. Similarly we have

$$\nu = \nu_{m_1} \dots \nu_{m_r} \cdot \nu_1 \quad \text{with} \quad {\nu_{m_i}}^{-1}\sigma_{m_i}\nu_{m_i} = {\sigma_{m_i}}^{p_i} \quad \text{and } \nu_1 \in S(\Omega_1).$$

It is clear that $p_i \equiv p \pmod{m_i}$. Since z commutes with ν we deduce that z_{m_i} commutes with ν_{m_i} for every i. Then we must have

$$\begin{aligned}
{\nu_{m_i}}^{-1} z_{m_i} \nu_{m_i} = z_{m_i} &\Rightarrow {\nu_{m_i}}^{-1} {\sigma_{m_i}}^{t_i} \nu_{m_i} = {\sigma_{m_i}}^{t_i} \\
&\Rightarrow ({\nu_{m_i}}^{-1}\sigma_{m_i}\nu_{m_i})^{t_i} = {\sigma_{m_i}}^{t_i} \\
&\Rightarrow {\sigma_{m_i}}^{p_i t_i} = {\sigma_{m_i}}^{t_i} \\
&\Rightarrow p_i t_i \equiv t_i \pmod{m_i} \\
&\Rightarrow (p_i - 1)t_i \equiv 0 \pmod{m_i}.
\end{aligned}$$

To be able to use Theorem 3.5.2 above to complete the proof, we need this equation to be true for every p_i coprime to m_i and for every t_i with $0 \leqslant t_i \leqslant m_i$.

Therefore we have to show that for every p_i coprime to m_i there exists p coprime to $|\sigma|$ for which ${\sigma_{m_i}}^{p_i}$ is a factor in σ^p written as a product of regular permutations. In other words, we need $\sigma^p|_{\Omega_{m_i}} = {\sigma_{m_i}}^{p_i}$. Now, since $|\sigma|$ is a multiple of m_i, say $|\sigma| = m_i a_i$, we can define a map f from $\mathbb{Z}_{m_i a_i}$ to $\mathbb{Z}_{m_i}$ by

$$f(x) = x \pmod{m_i}.$$

Since this map is a surjective homomorphism, then every invertible element of $\mathbb{Z}_{m_i}$ is the image of an invertible element of $\mathbb{Z}_{m_i a_i}$. i.e. the map f maps $U_{m_i a_i}$ onto U_{m_i}. This proves that for every p_i coprime to m_i there exists p with the above condition. Therefore the result follows by Theorem 3.5.2 above. □

Example 3.5.5 Let $\sigma = \sigma_3 \cdot \sigma_6 \cdot \sigma_8$ where σ_i is the product of disjoint i-cycles. Here $|\sigma| = 24$ and $\{1, 5, 7, 11, 13, 17, 19, 23\}$ is the set of numbers coprime to 24. The following shows the coprime powers of σ.

$$\begin{aligned}
\sigma^1 &= {\sigma_3}^1 \ {\sigma_6}^1 \ {\sigma_8}^1 \\
\sigma^5 &= {\sigma_3}^2 \ {\sigma_6}^5 \ {\sigma_8}^5 \\
\sigma^7 &= {\sigma_3}^1 \ {\sigma_6}^1 \ {\sigma_8}^7 \\
\sigma^{11} &= {\sigma_3}^2 \ {\sigma_6}^5 \ {\sigma_8}^3 \\
\sigma^{13} &= {\sigma_3}^1 \ {\sigma_6}^1 \ {\sigma_8}^5 \\
\sigma^{17} &= {\sigma_3}^2 \ {\sigma_6}^5 \ {\sigma_8}^1 \\
\sigma^{19} &= {\sigma_3}^1 \ {\sigma_6}^1 \ {\sigma_8}^3 \\
\sigma^{23} &= {\sigma_3}^2 \ {\sigma_6}^5 \ {\sigma_8}^7
\end{aligned}$$

Now

$$Z\big(N_{S_n}(\langle\sigma\rangle)\big) = \langle {\sigma_6}^3 \rangle \times \langle {\sigma_8}^4 \rangle \times Z\big(S(\Omega_1)\big). \qquad \square$$

As a result $Z(N)$ is isomorphic to $C_2 \times \cdots \times C_2$ where the number of C_2's depends on the size of Ω_1 and the number of different even cycles of different length in σ.

Example 3.5.6

$$Z\Big(N_{S_6}\big(\langle(1,2)(3,4)(5,6)\rangle\big)\Big) = \big\langle(1,2)(3,4)(5,6)\big\rangle \cong C_2.$$

$$Z\Big(N_{S_8}\big(\langle(1,2)(3,4)(5,6)\rangle\big)\Big) = \big\langle(1,2)(3,4)(5,6),(7,8)\big\rangle \cong C_2 \times S_2 \cong C_2 \times C_2.$$

Example 3.5.7 Let $\sigma = (1,2,3)(4,5)(6,7)$.Then

$$Z\Big(N_{S_7}\big(\langle\sigma\rangle\big)\Big) = \big\langle(4,5)(6,7)\big\rangle \cong C_2$$

$$Z\Big(N_{S_9}\big(\langle\sigma\rangle\big)\Big) = \big\langle(4,5)(6,7),(8,9)\big\rangle \cong C_2 \times S_2 \cong C_2 \times C_2.$$

Example 3.5.8

Let $\sigma = (1,2,3)(4,5,6)(7,8,9,10)(11,12,13,14)(15,16,17,18,19)$. Then

$$Z\Big(N_{S_{19}}\big(\langle\sigma\rangle\big)\Big) = \big\langle(7,9)(8,10)(11,13)(12,14)\big\rangle \cong Z\Big(N_{S_m}\big(\langle\sigma\rangle\big)\Big) \cong C_2$$

for $m = 20, 22, 23, 24, \ldots$. And

$$Z\Big(N_{S_{21}}\big(\langle\sigma\rangle\big)\Big) = \big\langle(7,9)(8,10)(11,13)(12,14),(20,21)\big\rangle \cong C_2 \times S_2 \cong C_2 \times C_2.$$

3.6 Is the Normaliser a Direct Product?

Let σ be a regular permutation which is a product of k disjoint m-cycles and let N be the normaliser of $\langle\sigma\rangle$ in S_{mk}. In the previous chapter we showed that the centraliser of a regular permutation σ is a direct product when $(m,k)=1$ (see Theorem 2.3.7). In the normaliser case we tried to find a similar result using GAP. In order to find all the direct factors of a group G we first calculate all the normal subgroups of G. For the following pairs of (m,k) we used Program 6.3.3 to find out whether N is a direct product. Experiments in GAP showed that for the following values of (m,k) the group N can be written as an internal direct product of two of its subgroups:

$(m,1)$ for $1 \leqslant m \leqslant 60$,

$(2,k)$ for $2 \leqslant k \leqslant 11$,

(3,2),(3,3),(3,4),(3,5),(3,6),(3,7),(3,8)

(4,2),(4,3),(4,4),(4,5),(4,6)

(5,2),(5,3),(5,4),(5,5),

(6,2),(6,3),(6,4),(6,5),

(7,2),(7,3),(7,4)

(8,2),(8,3),(8,4),

(9,2),(9,3),(9,4)

(10,2),(10,3),(10,4),

$(m,3)$ for $11 \leqslant m \leqslant 19$,

(20,2),(21,2) and (22,2).

When $k=1$ the permutation σ is an m-cycle and by Theorem 3.2.5

$$N_{S_m}(\langle\sigma\rangle) = U_m \ltimes C_m$$

with order $\phi(m)\cdot m$. GAP results tell us that for the following values of m the

normaliser is a direct product:

$$6, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 28, 30, 33, 34, 35, 36, 38, 39, 40, 42, 44, 45,$$
$$46, 48, 50, 51, 52, 54, 55, 56, 57, 58, 60.$$

This suggests the following theorem:

Theorem 3.6.1 If $m > 1$ is not a power of a prime then the normaliser of the subgroup generated by an m-cycle in S_m splits as a non-trivial direct product.

Proof:

If $m > 1$ is not a power of a prime, we can write $m = st$ with $s > 1, t > 1$ and $(s,t) = 1$. By Theorem 3.2.5, the normaliser of the subgroup generated by an m-cycle σ is

$$U_m \ltimes C_m = (U_s \times U_t) \ltimes (C_s \times C_t).$$

Then, as explained in Remark 5.2.1, $U_m = U_s \times U_t$ acts on $\mathbb{Z}_m = \mathbb{Z}_s \times \mathbb{Z}_t$. Then U_s acts trivially on $\mathbb{Z}_t$ and U_t acts trivially on $\mathbb{Z}_s$. So this semidirect product splits as a direct product of subgroups:

$$(U_s \ltimes C_s) \times (U_t \ltimes C_t). \qquad \square$$

Remark 3.6.2 The results of this theorem allow us to fill in the first column of Table 3.6.10 on page 78.

Example 3.6.3 Let $m = 15$ and $\sigma = (1, 2, \ldots, 15) \in S_{15}$. We write $15 = 3 \cdot 5$ with $s = 3$ and $t = 5$. The normaliser is the semidirect product $U_m \ltimes C_{S_m}(\sigma)$ by Theorem 3.2.5 which has order 120. Note that the centraliser of σ is just $\langle \sigma \rangle$. We get a copy of U_{15} in S_{15} as explained in the proof of Theorem 3.2.5 and

$$U_{15} = \{ h_t \mid (t, 15) = 1 \}.$$

The group of units of $\mathbb{Z}_{15}$ is:

$$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\} = \langle 11 \rangle \times \langle 7 \rangle \cong U_3 \times U_5$$

(we choose 11 and 7 because $11 \cdot 3 \equiv 3 \pmod{15}$ and $7 \cdot 5 \equiv 5 \pmod{15}$) and so the copy of U_{15} in S_{15} is isomorphic to $\langle h_{11} \rangle \times \langle h_7 \rangle$ where, by the definition of $U_m \subset S_m$, we have

$$h_{11} = (2,12)(3,8)(5,15)(6,11)(9,14),$$
$$h_7 = (2,8,5,14)(3,15,9,12)(4,7,13,10).$$

We get copies of C_3 and C_5 in S_{15} as follows:

$$C_3 = \langle \sigma^5 \rangle = \big\langle (1,6,11)(2,7,12)(3,8,13)(4,9,14)(5,10,15) \big\rangle \quad \text{and}$$
$$C_5 = \langle \sigma^3 \rangle = \big\langle (1,4,7,10,13)(2,5,8,11,14)(3,6,9,12,15) \big\rangle.$$

The action of $h_{11} \in U_3$ on C_5 (by conjugation) is trivial and similarly the action of $h_7 \in U_5$ on C_3 is also trivial and therefore we have

$$U_{15} \ltimes C_{15} = (U_3 \times U_5) \ltimes (C_3 \times C_5) = (U_3 \ltimes C_3) \times (U_5 \ltimes C_5).$$

$$H = U_3 \ltimes C_3 = \langle h_{11}, \sigma^5 \rangle, \qquad K = U_5 \ltimes C_5 = \langle h_7, \sigma^3 \rangle.$$

The order of H is $2 \cdot 3 = 6$ and the order of K is $4 \cdot 5 = 20$. □

Remark 3.6.4 Note that if m splits as a product of coprime divisors in more that one way, the group $N_{S_m}(\langle \sigma \rangle)$ also splits as a direct product in more than one way. For example if $m = 30$ the group $N_{S_{30}}(\langle \sigma \rangle)$ of order 240 splits as a direct product of a group of order h by another group of order k for (h,k) =(2,120),(6,40),(12,20).

In the case $m = 2$ the normaliser is isomorphic to the centraliser and we have a direct product when $k > 1$ is odd by Theorem 2.3.7. This allows us to fill in the top row of Table 3.6.10 on page 78.

In the case $k = 3$ we have a direct product for the following values of m:

$$2, 6, 10, 14, 18.$$

In each case the subgroup $\langle \sigma^{\frac{m}{2}} \rangle$ is a direct factor. Later results showed that the same result is true for the pairs $(6,5)$ and $(10,5)$. This suggests the following theorem:

Theorem 3.6.5 Let $m \equiv 2 \pmod 4$ and k be an odd number. Then the normaliser splits as a non-trivial direct product of its centre by another subgroup.

Proof:

Let Z be the centre of the normaliser. By Theorem 3.5.2 we have $Z = \langle \sigma^{\frac{m}{2}} \rangle$. Now we define a subgroup H of the normaliser in the following way. In the normaliser we have a copy of $C_m \times \cdots \times C_m$ (k-copies) which is generated by the m-cycles σ_i, i.e.

$$C_m \times \cdots \times C_m = \langle \sigma_1 \rangle \times \cdots \times \langle \sigma_k \rangle.$$

The set of even permutations of $C_m \times \cdots \times C_m$ are easily checked to be the following:

$$\{ {\sigma_1}^{a_1} \ldots {\sigma_k}^{a_k} \mid a_1 + \cdots + a_k \text{ is even } \}.$$

This is a subgroup of $C_m \times \cdots \times C_m$ which is isomorphic to

$$C_m \times \cdots \times C_m \times C_{\frac{m}{2}} \quad (k-1 \text{ copies of } C_m).$$

As we will discuss in Chapter 4, Theorem 4.2.1, this group is isomorphic to

$$\langle \sigma_1 \sigma_k \rangle \times \langle \sigma_2 \sigma_k \rangle \times \cdots \times \langle \sigma_{k-1} \sigma_k \rangle \times \langle {\sigma_k}^2 \rangle.$$

Now let H be the following subgroup of the normaliser:

$$H = U_m \ltimes \left(S_k \ltimes (C_m \times \cdots \times C_m \times C_{\frac{m}{2}}) \right).$$

The subgroup H has order $\frac{1}{2}\phi(m)k!m^k$ which has index 2 in the normaliser and so H is a normal subgroup of the normaliser. We will show that ZK, or equivalently $\langle Z, H \rangle$, is the normaliser. Note that H includes all the generators of the normaliser except σ_1. Now we show that we can obtain σ_1 from Z and H. Note that since $m \equiv 2 \pmod 4$ and k is odd

$$\tau = {\sigma_1}^{\frac{m}{2}+1} {\sigma_2}^{\frac{m}{2}} \ldots {\sigma_k}^{\frac{m}{2}}$$

is an element of H since the sum of the powers is even. Since $\sigma^{\frac{m}{2}} \cdot \tau = \sigma_1$, ZK is the normaliser. Since $|Z| \cdot |H|$ is equal to the order of the normaliser we have $Z \cap H = \{id\}$. Thus the result follows. □

Remark 3.6.6 In Chapter 5 we will show that when $m \equiv 2 \pmod 4$ all the elements of $U_m \subset S_{mk}$ will be even. We will also show that all the elements of the copy of S_k are even. Therefore H is isomorphic to the normaliser of σ in A_{mk}.

Remark 3.6.7 We have verified with GAP that certain other subgroups in the table do not split as direct products. These are indicated in Table 3.6.10 by N.

Remark 3.6.8 Using GAP we have verified that in the cases in Table 3.6.10 when $m \equiv 2 \pmod 4$ and k is odd that the normaliser can be written as a direct product in exactly four different ways. In each case $Z = \langle \sigma^{\frac{m}{2}} \rangle$ is a direct summand. If we denote the other direct summands by H_1, H_2, H_3, H_4, then we may take H_1 to be the subgroup we defined in the proof of above and we can get generators for these groups as follows:

$$H_1 = \langle u, \beta, \gamma, \sigma_1\sigma_k \rangle,$$
$$H_2 = \langle zu, z\beta, \gamma, \sigma_1\sigma_k \rangle,$$
$$H_3 = \langle zu, \beta, \gamma, \sigma_1\sigma_k \rangle,$$
$$H_4 = \langle u, z\beta, \gamma, \sigma_1\sigma_k \rangle.$$

where u is the generator of U_m (which is cyclic in all the cases examined), $z = \sigma^{\frac{m}{2}}$, β is the permutation which swaps first and second blocks, γ is the permutation which cyclically permutes the k blocks and σ_i is the i-th m-cycle in σ.

Note that to get a different direct summand from H_1 by multiplying a generator of H_1 by z, we must not multiply an element of odd order or else some power of this would be z and the intersection of two subgroups would be non-trivial. This is why we cannot multiply the generator γ by z to get a direct summand.

One may show that one may not multiply the generator $\sigma_1\sigma_k$ by z otherwise we get the whole group.

In the case $(m,k) = (6,3)$ we give the GAP output in Chapter 6, Program 6.3.3. We verified that in the output, by coincidence, the i-th printed subgroup is H_i.

Example 3.6.9 Let $m = 6$ and $k = 3$, then we may take σ to be the permutation

$$(1,2,3,4,5,6)(7,8,9,10,11,12)(13,14,15,16,17,18) \in S_{18}$$

and the normaliser is isomorphic to

$$U_6 \ltimes \left(S_3 \ltimes (C_6 \times C_6 \times C_6)\right)$$

which has order $2 \cdot 6 \cdot 6^3 = 2592$. Let $Z = \langle \sigma^3 \rangle$ be the centre of the normaliser. Let σ_i be the i-th cycle. Let

$$\begin{aligned} u &= (2,6)(3,5)(8,12)(9,11)(14,18)(15,17), \\ \beta &= (1,7)(2,8)(3,9)(4,10)(5,11)(6,12), \\ \gamma &= (1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18). \end{aligned}$$

In S_{18} we have:

$$U_6 = \langle u \rangle, \quad S_3 = \langle \beta, \gamma \rangle, \quad C_6 \times C_6 \times C_6 = \langle \sigma_1 \rangle \times \langle \sigma_2 \rangle \times \langle \sigma_3 \rangle.$$

Now we let H be the following group

$$\langle u, \beta, \gamma, \sigma_1\sigma_3 \rangle.$$

Note that other elements of the form $\sigma_i\sigma_j$ can be obtained by conjugating $\sigma_1\sigma_3$ by a suitable element of S_3. It is easy to verify that H contains

$$\{ {\sigma_1}^{a_1}{\sigma_2}^{a_2}{\sigma_3}^{a_3} \mid a_1 + a_2 + a_3 \text{ is even } \}.$$

This is isomorphic to

$$C_6 \times C_6 \times C_3 = \langle \sigma_1\sigma_3 \rangle \times \langle \sigma_2\sigma_3 \rangle \times \langle {\sigma_3}^2 \rangle.$$

So H is a subgroup of the normaliser of index 2. Now we show that $\langle Z, H \rangle$ is isomorphic to the normaliser. Note that

$$\tau = {\sigma_1}^4{\sigma_2}^3{\sigma_3}^3 \in H.$$

Since $\sigma^3 \cdot \tau = \sigma_1$ the generators of Z and H generate the normaliser and therefore we have a direct product.

GAP results show that the normaliser can be written as a direct product in 4 different ways. In each case the subgroup $\langle \sigma^3 \rangle$ (which is the centre) is a direct factor. The other subgroups are groups of order 1296. The centraliser is another normal subgroup of order 1296 but is not a direct factor. For details of these subgroups see the output of Program 6.3.3 for $m = 6, k = 3$. □

Among other values of m and k we found that the normaliser is a direct product for $(m, k) = (3, 2)$. In this case $\sigma = (1, 2, 3)(4, 5, 6) \in S_6$. The normaliser is isomorphic to

$$U_3 \ltimes (C_3 \wr S_2) = U_3 \ltimes \left(S_2 \ltimes (C_3 \times C_3)\right)$$

with order $2 \cdot 2 \cdot 3^2 = 36$. In S_6 we have copies of $U_3 \cong C_2, S_2$ and $C_3 \times C_3$ as follows:

$$\begin{aligned} U_3 \cong C_2 &= \big\langle (2, 3)(5, 6) \big\rangle, \\ S_2 &= \big\langle (1, 4)(2, 5)(3, 6) \big\rangle, \\ C_3 \times C_3 &= \big\langle (1, 2, 3), (4, 5, 6) \big\rangle, \end{aligned}$$

and the normaliser can be generated by these subgroups. Since 2 and 3 are coprime, by Theorem 2.3.7 the centraliser is the direct product $\langle \sigma \rangle \times H$ where H is the normal closure of the copy of S_2 in the centraliser and in this case (by the

proof of Theorem 2.3.7) we have

$$H = \langle (1,2,3)(4,6,5), (1,4)(2,5)(3,6) \rangle$$

with order 6 and isomorphic to S_3. Therefore the normaliser is isomorphic to

$$U_3 \ltimes (C_3 \times S_3).$$

Let K be the subgroup of S_6 given by

$$K = \langle (1,2,3)(4,5,6), (1,4)(2,6)(3,5) \rangle \cong S_3.$$

The generators of K normalise $\langle \sigma \rangle$ and hence this is a subgroup of $N_{S_6}(\langle \sigma \rangle)$. We can write $(2,3)(5,6)$ as the product of $(1,4)(2,5)(3,6)$ and $(1,4)(2,6)(3,5)$ and so H and K generate the whole of the normaliser. Since one can easily verify that both H and K are normal subgroups with $H \cap K = \{ id \}$ we have:

$$N_{S_6}(\langle \sigma \rangle) = H \times K \cong S_3 \times S_3.$$

The following table summarises the results of this section. In the table, a "$\times$" marks those which are non-trivial direct products; a "N" marks those for which we do not have a direct product and spaces marks those for which we do not know the answer.

TABLE: 3.6.10

m \ k	1	2	3	4	5	6	7	8	9	10	11
2	N	N	×	N	×	N	×	N	×	N	×
3	N	×	N	N	N	N	N	N			
4	N	N	N	N	N	N					
5	N	N	N	N	N						
6	×	N	×	N	×		×		×		×
7	N	N	N	N							
8	N	N	N	N							
9	N	N	N	N							
10	×	N	×	N	×		×		×		×
11	N	N	N								
12	×	N	N								
13	N	N	N								
14	×	N	×		×		×		×		×
15	×	N	N								
16	N	N	N								
17	N	N	N								
18	×	N	×		×		×		×		×
19	N	N	N								
20	×	N									
21	×	N									
22	×	N	×		×		×		×		×

Chapter 4

Centralisers in A_n

4.1 Introduction

Let $\sigma \in S_n$. In this chapter we investigate the elements of A_n which commute with σ. In other words we find the even elements of $C_{S_n}(\sigma)$. Note that σ need not be even to define the centraliser:

$$C_{A_n}(\sigma) = \{ x \in A_n \mid x^{-1}\sigma x = \sigma \}.$$

We show that when σ is regular, $C_{A_n}(\sigma)$ is either a wreath product or a different semidirect product. In general case we show that the direct product of the centralisers of the regular parts of σ is a normal subgroup of the centraliser of σ. We give the conditions (for both regular and general case) for which $C_{S_n}(\sigma) = C_{A_n}(\sigma)$.

4.2 Regular Case

We have the following result.

Theorem 4.2.1 Let $\sigma \in S_{mk}$ be a product of k disjoint m-cycles. If m is even then

$$C_{A_{mk}}(\sigma) \cong S_k \ltimes (C_m \times \ldots \times C_m \times C_{\frac{m}{2}}) \quad (k-1 \text{ copies of } C_m).$$

If m is odd then

$$C_{A_{mk}}(\sigma) \cong C_m \wr A_k.$$

Proof:

Let

$$\sigma = (1, 2, \ldots, m)(m+1, \ldots, 2m) \ldots \big((k-1)m+1, \ldots, km\big).$$

By Section 2.3, $C_{S_{mk}}(\sigma)$ is generated by the following three permutations:

$$\begin{aligned}
\alpha &= (1, 2, \ldots, m), \\
\beta &= (1, m+1)(2, m+2) \ldots (m, 2m), \\
\gamma &= \big(1, m+1, \ldots, (k-1)m+1\big) \ldots (m, 2m, \ldots, km).
\end{aligned}$$

We examine the two cases in the statement of the theorem separately.

<u>**Case 1:**</u> The cycle length m is even.

In this case α is odd, β and γ are even. Since an element of $C_{S_{mk}}(\sigma)$ can be written as

$$[h'; c_1, c_2, \ldots, c_k] \text{ where } h' \in S_k \text{ and } c_i \in C_m$$

and S_k is generated by $\{\beta, \gamma\}$ we see that even elements of $C_{S_{mk}}(\sigma)$ come from the even elements of

$$C_m \times C_m \times \ldots \times C_m \quad (k\text{-copies}).$$

Now we find the even elements of the direct product.

Let $\sigma = \sigma_1\sigma_2\ldots\sigma_k$ where σ_i is the i-th m-cycle. Then:

$$C_m \times C_m \times \ldots \times C_m = \langle\sigma_1\rangle \times \ldots \times \langle\sigma_k\rangle$$

Consider the function

$$\varphi : C_m \times \ldots \times C_m \longrightarrow C_m \times \ldots \times C_m$$

defined, on the generators, by multiplication (on the right) by σ_k. The map φ is clearly a homomorphism with $\mathrm{Ker}(\varphi) = \langle {\sigma_k}^{\frac{m}{2}}\rangle$ of order 2. Notice that $\mathrm{Im}(\varphi)$ consists of only even elements. If a permutations group G contains odd elements then the subgroup of even elements of G has order $\frac{|G|}{2}$. It follows that the subgroup of even elements of $C_m \times \ldots \times C_m$ are isomorphic to

$$\mathrm{Im}(\varphi) = C_m \times \ldots \times C_m \times C_{\frac{m}{2}} \quad (k-1 \text{ copies of } C_m)$$

which is generated by:

$$\{\sigma_1\sigma_k, \ldots, \sigma_{k-1}\sigma_k, {\sigma_k}^2\}.$$

So we have:

$$C_{A_{mk}}(\sigma) \cong S_k \ltimes (C_m \times \ldots \times C_m \times C_{\frac{m}{2}}) \quad (k-1 \text{ copies of } C_m).$$

An element of S_k in $C_{A_{mk}}(\sigma)$ which leaves the last block fixed acts on the blocks of $C_{A_{mk}}(\sigma)$ in the same way as on the blocks of $C_{S_{mk}}(\sigma)$. That is, we have a subgroup of $C_{A_{mk}}(\sigma)$ which is a wreath product, namely $C_m \wr S_{k-1}$. In general this subgroup is not normal and the index of this subgroup is $km/2$. The group $C_{A_{mk}}(\sigma)$ is a normal subgroup of $C_{S_{mk}}(\sigma)$ of index 2. The coset representatives can be taken as id and α.

<u>Case 2:</u> The cycle length m is odd.

In this case α is even, β is odd ($\beta = id$ when $k = 1$) and γ has the opposite parity to k (except when $k = 1$). Since an element of $C_{S_{mk}}(\sigma)$ can be written as

$$[h'; c_1, c_2, \ldots, c_k] \text{ where } h' \in S_k \text{ and } c_i \in C_m$$

and $C_m \times \ldots \times C_m \subset S_{mk}$ is generated by even elements, we see that even elements of $C_{S_{mk}}(\sigma)$ come from even block transformations. Therefore

$$C_{A_{mk}}(\sigma) \cong C_m \wr A_k$$

and if $k > 1$ (see remark below for case $k = 1$) then $C_{A_{mk}}(\sigma)$ has two cosets in $C_{S_{mk}}(\sigma)$ and is therefore normal. Coset representatives can be taken as id and β.

Remark 4.2.2 If m is odd and $k = 1$ then $\sigma = (1, 2, \ldots, m)$ and $C_{S_m}(\sigma) = \langle\sigma\rangle$. Since σ is even $\langle\sigma\rangle \subset A_m$, therefore:

$$C_{S_m}(\sigma) = C_{A_m}(\sigma) \cong C_m$$

and this is the only case where $C_{S_{mk}}(\sigma) = C_{A_{mk}}(\sigma)$.

Remark 4.2.3 Note that although A_2 is trivial as an abstract group, it still acts on a 2-element set and so the permutation wreath product $C_m \wr A_2$ has order m^2.

Example 4.2.4 Let $\sigma = (1,2,3,4)(5,6,7,8)(9,10,11,12)$. The group $C_{A_{12}}(\sigma)$ has order $192 = \frac{3!\cdot 4^3}{2}$ and is generated by:
$\{(1,5)(2,6)(3,7)(4,8), (1,5,9)(2,6,10)(3,7,11)(4,8,12),$
$(1,2,3,4)(9,10,11,12), (5,6,7,8)(9,10,11,12), (9,11)(10,12)\}$.

This group is a normal subgroup of $C_{S_{12}}(\sigma)$ of index 2. Coset representatives can be taken as id and $\alpha = (1,2,3,4)$.

This group has a subgroup isomorphic to $C_4 \wr S_2$ which is generated by:

$$\{(1,2,3,4)(9,10,11,12), (1,5)(2,6)(3,7)(4,8)\}.$$

Example 4.2.5 Let $\sigma = (1,2,3)(4,5,6)(7,8,9)(10,11,12)$. Then $C_{A_{12}}(\sigma)$ has order $972 = \frac{4!\cdot 3^4}{2}$ and is generated by:

$$\{(1,2,3), (1,4,7)(2,5,8)(3,6,9), (1,4,10)(2,5,11)(3,6,12)\}.$$

This group is a normal subgroup of $C_{S_{12}}(\sigma)$ of index 2. Coset representatives can be taken as id and $\beta = (1,4)(2,5)(3,6)$.

Example 4.2.6 Let $\sigma = (1,2,3,4,5,6,7,8,9)$. Then

$$C_{A_9}(\sigma) = C_{S_9}(\sigma) = \langle \sigma \rangle \cong C_9.$$

4.3 General Case

Let $\sigma \in S_n$ be a product of regular permutations. We define the σ_{m_i}'s, the Ω_{m_i}'s and r as in Theorem 2.2.1.

We begin by examining an example.

Example 4.3.1 Let

$\sigma = (1,2,3)(4,5,6)(7,8,9,10)(11,12,13,14)(15,16,17,18,19)(20,21,22,23,24)$

with:

$\sigma_3 = (1,2,3)(4,5,6)$,

$\sigma_4 = (7,8,9,10)(11,12,13,14)$,

$\sigma_5 = (15,16,17,18,19)(20,21,22,23,24)$

so that $\sigma = \sigma_3 \cdot \sigma_4 \cdot \sigma_5$. Theorem 4.2.1 above gives the following results:

$$\begin{aligned} |C_{A(\Omega_3)}(\sigma_3)| &= 9, \\ |C_{A(\Omega_4)}(\sigma_4)| &= 16, \\ |C_{A(\Omega_5)}(\sigma_5)| &= 25. \end{aligned}$$

A calculation in GAP gives

$$|C_{A_{24}}(\sigma)| = 14400 = 4 \cdot (9 \cdot 16 \cdot 25).$$

Using GAP we verified that the direct product of centralisers of the σ_{m_i}'s is a subgroup of the centraliser of σ, in this case of index 4. To see why the subgroup is proper, observe that we can have an even element which conjugates σ_3 into itself, and two odd elements which conjugate σ_4 into σ_4 and σ_5 into σ_5. Their product is even and so is an element of $C_{A_{24}}(\sigma)$. From the following table we see that there are four ways to get an even element.

1. Even $\times$ Even $\times$ Even : 3600 of them
2. Even $\times$ Odd $\times$ Odd : 3600 of them
3. Odd $\times$ Even $\times$ Odd : 3600 of them
4. Odd $\times$ Odd $\times$ Even : 3600 of them

In total 14400 even elements conjugate σ into itself, while only those in the first row of the table come from the product of the centralisers in $A(\Omega_{m_i})$ of σ_{m_i}. Notice also that if σ had an extra copy of an m-cycle where $m = 7, 9, 11, \ldots$, then we would not get an odd element from its centraliser. Consideration of examples like that above leads to the following result.

Theorem 4.3.2 Let $\sigma \in S_n$ be a product of regular permutations as in Theorem 2.2.1. Then:

$$C_{A(\Omega_{m_1})}(\sigma_{m_1}) \times \ldots \times C_{A(\Omega_{m_r})}(\sigma_{m_r}) \trianglelefteq C_{A_n}(\sigma).$$

Let

$$r_1 = r - (\text{number of } i \text{ for which } k_{m_i} = 1 \text{ and } m_i \text{ is odd}).$$

If $r_1 = 0$ or 1 then the groups are isomorphic. Otherwise the subgroup has index 2^{r_1-1}.

Proof:

Let $G_{m_i} = C_{A(\Omega_{m_i})}(\sigma_{m_i})$. An element of $G_{m_1} \times \ldots \times G_{m_r}$ is even and clearly conjugates σ into itself, so

$$G_{m_1} \times \ldots \times G_{m_r} \leqslant C_{A_n}(\sigma).$$

Let $x \in G_{m_1} \times \ldots \times G_{m_r}$ and $h \in C_{A_n}(\sigma)$. Then $x = x_{m_1} \ldots x_{m_r}$ with x_{m_i} acting on Ω_{m_i} and ${x_{m_i}}^{-1}\sigma_{m_i}x_{m_i} = \sigma_{m_i}$. We also have $h = h_{m_1} \ldots h_{m_r}$ with h_{m_i} acting on Ω_{m_i} and ${h_{m_i}}^{-1}\sigma_{m_i}h_{m_i} = \sigma_{m_i}$. Note that h_{m_i} need not be even but the x_{m_i} is even. Then:

$$\begin{aligned} h^{-1}xh &= ({h_{m_1}}^{-1}x_{m_1}h_{m_1}) \ldots ({h_{m_r}}^{-1}x_{m_r}h_{m_r}) \\ &= t_1t_2 \ldots t_r \qquad (\text{by letting} \quad t_i = {h_{m_i}}^{-1}x_{m_i}h_{m_i}). \end{aligned}$$

Now t_i is even since it is a conjugate of x_{m_i} and clearly $t_i \in G_{m_i}$. So $x^{-1}hx$ is an element of the direct product and so the subgroup is normal.

Now we prove that the index is as stated in the theorem. If $r_1 = 0$ then $k_{m_i} = 1$ and m_i is odd for every i. By Remark 4.2.2, h_{m_i} is even and is an element of $\langle \sigma_{m_i} \rangle$. So we have

$$|C_{A_n}(\sigma)| = m_1 \dots m_r = |C_{S_n}(\sigma)|$$

which is equal to the product of sizes of centralisers of σ_{m_i}'s. In this case

$$C_{A_n}(\sigma) = C_{S_n}(\sigma).$$

If $r_1 = 1$ then for only one i (say for $i = 1$) either $k_{m_1} > 1$ or $k_{m_1} = 1$ with m_1 even. In this case h_{m_1} must be even since other h_{m_i}'s are all even. Therefore $h \in G_{m_1} \times \cdots \times G_{m_r}$ and we have an isomorphism. Note that if a permutation group $G \subset S_n$ contains an odd permutation σ, then $G \cap A_n$ has cosets $G \cap A_n$ and $\sigma(G \cap A_n)$ in G and so has index 2. Since $C_{S(\Omega_{m_1})}(\sigma_{m_1})$ includes odd elements, we have

$$|C_{A_n}(\sigma)| = \frac{|C_{S_n}(\sigma)|}{2}.$$

If $r_1 > 1$ then we still have the above equation. Now if σ_{m_j} is a regular permutation for which either $k_{m_j} > 1$ or $k_{m_j} = 1$ with m_j even, then we have

$$|C_{A(\Omega_{m_j})}(\sigma_{m_j})| = \frac{k_j! \cdot {m_j}^{k_j}}{2}.$$

So,

$$|G_{m_1} \times \ldots \times G_{m_r}| = \frac{|C_{S_n}(\sigma)|}{2^{r_1}}$$

which shows that the index is $2^{r_1 - 1}$. □

Remark 4.3.3 If σ has fixed points then the contribution of the centraliser of the product of 1-cycles σ_1 on Ω_1 is $A(\Omega_1)$ with order $\frac{1}{2}|\Omega_1|!$ except when $|\Omega_1| = 1$, when the group is trivial.

Example 4.3.4 Let

$\sigma = (1,2,3)(4,5,6,7,8)(9,10,11,12,13,14,15)(16,17,18,19,20,21,22,23,24)$

with

$\sigma_3 = (1,2,3)$,

$\sigma_5 = (4,5,6,7,8)$,

$\sigma_7 = (9,10,11,12,13,14,15)$,

$\sigma_9 = (16,17,18,19,20,21,22,23,24)$.

Now, $|C_{A(\Omega_i)}(\sigma_i)| = i$ for $i = 3,5,7,9$ and

$$|C_{A_{24}}(\sigma)| = |C_{S_{24}}(\sigma)| = 945 = 3 \cdot 5 \cdot 7 \cdot 9.$$

This shows that

$$C_{A_{24}}(\sigma) \cong C_{A(\Omega_3)}(\sigma_3) \times C_{A(\Omega_5)}(\sigma_5) \times C_{A(\Omega_7)}(\sigma_7) \times C_{A(\Omega_9)}(\sigma_9).$$

Example 4.3.5 Let

$\sigma = (1,2)(3,4)(5,6,7)(8,9,10)(11,12,13)(14,15,16,17)(18,19,20,21,22)$

with

$\sigma_2 = (1,2)(3,4)$,

$\sigma_3 = (5,6,7)(8,9,10)(11,12,13)$,

$\sigma_4 = (14,15,16,17)$,

$\sigma_5 = (18,19,20,21,22)$.

We have the following results

$$\begin{aligned} |C_{A(\Omega_2)}(\sigma_2)| &= 4, \\ |C_{A(\Omega_3)}(\sigma_3)| &= 81, \\ |C_{A(\Omega_4)}(\sigma_4)| &= 2, \\ |C_{A(\Omega_5)}(\sigma_5)| &= 5, \\ |C_{A_{22}}(\sigma)| &= 12960 = 4 \cdot (4 \cdot 81 \cdot 2 \cdot 5). \end{aligned}$$

This shows that the direct product of the centralisers of regulars parts is a subgroup of the centraliser of σ in A_{22} of index 4. Notice that $r = 4$, $r_1 = 4-1 = 3$ and $2^{r_1-1} = 4$ which is the index.

Example 4.3.6 Let

$\sigma = (1,2,3)(4,5,6,7)(8,9,10,11)(12,13,14,15,16)(17,18,19,20,21,22,23)$

with

$\sigma_3 = (1,2,3)$,

$\sigma_4 = (4,5,6,7)(8,9,10,11)$,

$\sigma_5 = (12,13,14,15,16)$,

$\sigma_7 = (17,18,19,20,21,22,23)$.

We have the following results

$$\begin{aligned} |C_{A(\Omega_3)}(\sigma_3)| &= 3, \\ |C_{A(\Omega_4)}(\sigma_4)| &= 16, \\ |C_{A(\Omega_5)}(\sigma_5)| &= 5, \\ |C_{A(\Omega_7)}(\sigma_7)| &= 7, \\ |C_{A_{23}}(\sigma)| &= 1680 = 3 \cdot 16 \cdot 5 \cdot 7. \end{aligned}$$

This shows that the direct product of the centralisers of regulars parts is isomorphic to the centraliser of σ in A_{23}. Notice that $r = 4$, $r_1 = 4-3 = 1$ and $2^{r_1-1} = 1$ which is the index.

Chapter 5

Normalisers of Cyclic Subgroups in A_n

5.1 Introduction

In this chapter we investigate the normaliser in A_n of a subgroup of S_n which is generated by $\sigma \in S_n$. Notice that it still makes sense to define the normaliser if σ is not an element of A_n.

$$N_{A_n}(\langle\sigma\rangle) = \{\, x \in A_n \mid x^{-1}\langle\sigma\rangle x = \langle\sigma\rangle \,\}.$$

First we examine the regular case. The structure of the normaliser in A_n is more complicated than that of the normaliser in S_n. The action of $U_m = \mathrm{Aut}(C_m)$ as a permutation group on C_m plays an important role and we give an interesting result which gives the conditions for which all the elements of U_m act as even permutations. We determine the structure of the normaliser for all possible cases and show them in a table.

In the general case we analyse how the normaliser of $\langle\sigma\rangle$ and the direct product of the normalisers of the subgroups generated by the regular parts are related.

We give necessary and sufficient conditions (for both regular and general case) for which $N_{S_n}(\langle\sigma\rangle) = N_{A_n}(\langle\sigma\rangle)$.

5.2 Regular Case

Assume for the moment that σ is a regular permutation which is a product of k disjoint m-cycles. We know from Theorem 3.2.5 that

$$N_{S_{mk}}(\langle\sigma\rangle) \cong U_m \ltimes (C_m \wr S_k).$$

Equivalently, an element of $N_{S_{mk}}(\langle\sigma\rangle)$ can be uniquely expressed as

$$[u'; h'; c_1, c_2, \ldots, c_k] \text{ where } u' \in U_m, h' \in S_k \text{ and } c_i \in C_m.$$

In the previous chapters we have illustrated how to obtain these groups in S_{mk}. For example if :
$\sigma = (1,2,3)(4,5,6)(7,8,9)(10,11,12) \in S_{12}$ then, $m = 3, k = 4$. Then we have the following subgroups of S_{12}:

$$\langle (1,4)(2,5)(3,6), (1,4,7,10)(2,5,8,11)(3,6,9,12) \rangle$$

which is isomorphic to S_4,

$$\langle (1,2,3), (4,5,6), (7,8,9), (10,11,12) \rangle$$

which is isomorphic to $C_3 \times C_3 \times C_3 \times C_3$, and

$$\langle (2,3)(5,6)(8,9)(11,12) \rangle$$

which is a cyclic group of order 2 and isomorphic to $U_3 = \mathrm{Aut}(C_3)$.

As in the proof of Theorem 3.2.5 we identify U_m with those elements of S_{mk} which conjugate σ into σ^t for some t such that $(t, m) = 1$ and fix the set F (in the above example $F = \{1, 4, 7, 10\}$). We shall investigate under what circumstances all the elements of U_m are even.

If k is even, then by the construction of $U_m \subset S_{mk}$ in the proof of Theorem 3.2.5 a permutation in $U_m \subset S_{mk}$ is a product of k permutations and these

permutations have the same cycle shape. Therefore all the permutations in U_m are even.

When k is odd the situation is more complicated. To see what can happen in this case, we examine in more detail the case $k = 1$. In this case, U_m is a subgroup of S_m and it will be convenient to think of it as acting on the set $\mathbb{Z}_m$ which we take to be $\{0, 1, \ldots, m-1\}$. The action of an element $t \in U_m$ may be regarded as multiplication by t (modulo m). Note that this fixes the "first" element 0 of $\mathbb{Z}_m$.

For example if $m = 9, t = 5$ this is the permutation

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 5 & 1 & 6 & 2 & 7 & 3 & 8 & 4 \end{pmatrix} = (1,5,7,8,4,2)(3,6)$$

which is even. If we take $m = 5$ and $t = 3$ then we get the permutation

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 3 & 1 & 4 & 2 \end{pmatrix} = (1,3,4,2)$$

which is odd. For some values of m, we get even permutations for every element of U_m. A program written in GAP (see Program 6.3.1) gives us a list of such numbers m as follows:

$$2, 6, 9, 10, 14, 18, 22, 25, 26, 30, 34, 38, 42, 46, 49, \ldots$$

This suggests that $m \equiv 2 \pmod 4$ or m is an odd square. We give a proof of this result in the following theorem. We now give the following remark which will be used in the theorem.

Remark 5.2.1 If s, t are coprime then the rings $\mathbb{Z}_{st}$ and $\mathbb{Z}_s \times \mathbb{Z}_t$ are isomorphic. We prefer to choose an isomorphism mapping $(1,1) \in \mathbb{Z}_s \times \mathbb{Z}_t$ to $1 \in \mathbb{Z}_{st}$. To do this choose $p, q \in \mathbb{Z}$ such that

$$ps + qt = 1$$

and then a suitable isomorphism is given by

$$(x, y) \longmapsto psy + qtx \pmod{st}, \quad \text{for } (x, y) \in \mathbb{Z}_s \times \mathbb{Z}_t.$$

Under this isomorphism, the set $U_s \times U_t$ of units in $\mathbb{Z}_s \times \mathbb{Z}_t$ is mapped to the units U_{st} in $\mathbb{Z}_{st}$. We may think of this in the following way. Think of $\mathbb{Z}_{st}$ as an $s \times t$ array where the $\mathbb{Z}_s$ labels the rows and $\mathbb{Z}_t$ labels the columns. Then the action of U_{st} on the elements of this array will be that induced by the action of U_s on rows and U_t on columns.

We give an example to illustrate the above. Let $s = 5, t = 8$. We have

$$1 = -3 \cdot 5 + 2 \cdot 8$$

and the map

$$f : \mathbb{Z}_5 \times \mathbb{Z}_8 \longrightarrow \mathbb{Z}_{40}$$

is given by

$$f(x, y) = 16x - 15y = 16x + 25y \pmod{40}.$$

In the following table the entry (i, j) is $f(i, j)$ for $0 \leqslant i \leqslant 4, 0 \leqslant j \leqslant 7$ and the elements of U_{40} are framed.

	[1]	2	[3]	4	[5]	6	[7]	0
[1]	[1]	26	[11]	36	[21]	6	[31]	16
[2]	[17]	2	[27]	12	[37]	22	[7]	32
[3]	[33]	18	[3]	28	[13]	38	[23]	8
[4]	[9]	34	[19]	4	[29]	14	[39]	24
0	0	25	10	35	20	5	30	15

For example, the action of $13 = f(3, 5) \in U_{40}$ on $\mathbb{Z}_{40}$ is given by the action of $3 \in U_5$ on rows and $5 \in U_8$ on columns. The actions of 3 on $\mathbb{Z}_5$ and 5 on $\mathbb{Z}_8$ are given by the permutations $\alpha = (1, 3, 4, 2)$ and $\beta = (1, 5)(3, 7)$ respectively. The

action of 13 on C_{40} can be given by the formula:

$$(x, y) \longmapsto (x\alpha, y\beta).$$

This action corresponds to the multiplying elements of the array by 13 modulo 40. For instance $1 = f(1,1)$ is moved to $13 = f(3,5) = f(1\alpha, 1\beta)$.

Theorem 5.2.2 Suppose that $U_m = \mathrm{Aut}(C_m)$ acts on $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ by multiplication. All the permutations produced in this way are even if and only if m is an odd square or $m \equiv 2 \pmod 4$.

Proof:

We first consider the case when p is an odd prime and $m = p^2$. Then $|U_m| = \phi(m) = p^2 - p$ and U_m is a cyclic group with generator, say k. The group U_m acts on $\mathbb{Z}_m$ by multiplication and multiplication by the element k permutes the invertible elements U_m of $\mathbb{Z}_m$ among themselves as a $(p^2 - p)$-cycle. This permutation is therefore an even length cycle and so is an odd permutation. The rest of $\mathbb{Z}_m$ consists of the 0-element and $p - 1$ other elements which are divisible by p but not by p^2. Multiplication by k fixes the 0-element and permutes the other $p - 1$ elements among themselves as a $(p-1)$-cycle. Again, since p is odd, this is an even length cycle and so is odd. Thus the action of k is given as the product of two odd permutations and thus is an even permutation. Thus the action of every element is via an even permutation.

For example, if $p = 5$, then U_{25} may be generated by (among other elements) 2. (The other primitive roots are $3, 8, 12, 13, 17, 22, 23$). The element 2 acts on the set $\{0, 1, \ldots, 24\}$ as the permutation

$$(0)(1, 2, 4, 8, 16, 7, 14, 3, 6, 12, 24, 23, 21, 17, 9, 18, 11, 22, 19, 13)(5, 10, 20, 15)$$

which is a product of a 4-cycle and a 20-cycle and hence is an even permutation. Other elements of U_{25} are powers of 2 and hence also act as even permutations.

For example, multiplication by 11 produces the permutation

$$(1,11,21,6,16)(2,22,17,12,7)(3,8,13,18,23)(4,19,9,24,14)(5)(10)(15)(20)$$

which is again even.

We now look at the case when m is a power of an odd prime, $m = p^r$, say. By the theory of the primitive element, U_m is cyclic with generator k, say. We will show by induction on r that multiplication by k produces a permutation of $\mathbb{Z}_m$ which is a product of cycles of lengths

$$(p^r - p^{r-1}), (p^{r-1} - p^{r-2}), \ldots, (p^2 - p), (p-1), 1.$$

We note that $\mathbb{Z}_{p^r} = U_m \cup p\mathbb{Z}_{p^{r-1}}$. The element k permutes the elements of U_m cyclically and since $k \pmod{p^{r-1}}$ is a generator of $U_{p^{r-1}}$, by the inductive hypothesis, k acts on $p\mathbb{Z}_{p^{r-1}}$ as a product of cycles of lengths

$$(p^{r-1} - p^{r-2}), (p^{r-2} - p^{r-3}), \ldots, (p^2 - p), (p-1), 1.$$

This completes the case when $m = p^r$.

Hence the multiplication by k on $\mathbb{Z}_{p^r}$ produces a product of r even length cycles and so is an even permutation if and only if r is even. Thus if $m = p^r$, all the permutations are even if and only if m is a perfect square.

Next we look at the case when m is odd and not a power of a prime. As in Remark 5.2.1 we write $m = st$ with $(s,t) = 1$ and think of $U_{st} = U_s \times U_t$ acting on the array $\mathbb{Z}_s \times \mathbb{Z}_t$ via the action on rows and columns. Note that both s and t are odd. Then the action on rows by an element of U_s which corresponds to a transposition, swaps t elements in the array and so is a product of t transpositions and hence is an odd permutation. Hence odd permutations in U_s act as odd permutations on $\mathbb{Z}_{st}$ and even permutations act as even permutations on $\mathbb{Z}_{st}$. Similarly for odd and even permutations in U_t.

Suppose m is odd, but is not a square. Then m is divisible by an odd power of a prime p, say $m = p^r t$ with p, t coprime. In the above, take $s = p^r$ and then U_s has an odd permutation by the earlier case and so U_{st} has an odd permutation.

Suppose m is odd and is a square, then:

$$m = {p_1}^{r_1} \cdot {p_2}^{r_2} \ldots {p_t}^{r_t}$$

where the p_i's are odd primes and the r_i's are even. Then

$$m = {p_1}^{r_1} \cdot t \quad \text{(where } t \text{ is an odd square).}$$

By the above argument, ${p_1}^{r_1}$ gives even permutations. Since ${p_1}^{r_1}$ and t are coprime, by induction, it is easy to prove that m produces even permutations.

The final case we consider is with m even. If 4 divides m, say $m = 4k$, then multiplication by -1 is a product of $(2k-1)$ 2-cycles and so is odd. If 4 does not divide m then $m = 2t$ with $2, t$ coprime. Since $U_2 = id$, this acts trivially on rows. Any transposition of U_t gives an even permutation of the whole set and so permutations are even and the result follows. □

We may restate this theorem as a result about conjugation of an m-cycle.

Corollary 5.2.3 If m is an odd square then a permutation in S_m which conjugates an m-cycle σ into σ^t with $(t, m) = 1$, is even. If $m \equiv 2 \pmod 4$ then a permutation in S_m which conjugates an m-cycle σ into $\sigma^t, (t, m) = 1$, and fixes at least one of the symbols, is even.

Proof:

Let m be an odd square. Then

$$N_{S_m}(\langle\sigma\rangle) = U_m \ltimes C_{S_m}(\sigma).$$

From Theorem 5.2.2, all the elements of U_m are even and by Remark 4.2.2, every element in $C_{S_m}(\sigma)$ is even and thus $N_{A_m}(\langle\sigma\rangle)$ consists only of even elements and so $N_{S_m}(\langle\sigma\rangle) = N_{A_m}(\langle\sigma\rangle)$.

If $m \equiv 2 \pmod 4$ and τ conjugates σ into σ^t fixing (say) a_0, then we may write $\sigma = (a_0, a_1, \ldots, a_{m-1})$ and the action of τ is the same as the action of $t \in U_m$ on the subscripts. Thus τ is even from the theorem. □

Remark 5.2.4 The condition about fixing an element in the even case is necessary since if σ is a $(4k+2)$-cycle, then $\tau = \sigma$ conjugates σ into itself, but is an odd permutation.

Let σ be a regular permutation which is a product of k disjoint m-cycles. From Chapter 4 we know that if m is even or $k > 1$ then the centraliser of σ in S_{mk} includes odd permutations. Again from Chapter 4 we know that if m is odd and $k = 1$ then all the elements of the centraliser in S_m of $\sigma = (1, 2, \ldots, m)$ are even and this is the only case where the centraliser of a regular permutation in S_{mk} is the same as the centraliser in A_{mk}. Since the above Theorem 5.2.2 shows that when $k = 1$ and m is an odd square, all the elements of $U_m \subset S_m$ are even, we deduce the following corollary.

Corollary 5.2.5 Let σ be a regular permutation which is a product of k disjoint m-cycles, then:

$N_{S_{mk}}(\langle\sigma\rangle) = N_{A_{mk}}(\langle\sigma\rangle)$ if and only if m is an odd square and $k = 1$. □

Example 5.2.6 Let $\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9)$, then

$$N_{A_9}(\langle\sigma\rangle) = N_{S_9}(\langle\sigma\rangle) \cong U_9 \ltimes C_9 \text{ with order } 54.$$ □

We determined that if m is an odd square or $m \equiv 2 \pmod 4$ or k is even then all the elements of $U_m \subset S_{mk}$ are even. An element ν of the normaliser can be written as

$$\nu = [u'; h'; c_1, \ldots, c_k] \quad \text{where } u' \in U_m \subset S_{mk}, h' \in S_k \subset S_{mk}, c_i \in C_m.$$

To determine the normaliser we have to consider several cases. For the value of m we consider the following cases: m an odd square, m odd but not an odd

square, $m \equiv 2 \pmod 4$ and $m \equiv 0 \pmod 4$. For the value of k the cases to be considered are: $k = 1$, $k > 1$ odd and k even. From Chapter 4 and from the results of this chapter we have the following:

1. All the elements of $U_m \subset S_{mk}$ are even if and only if m is an odd square or $m \equiv 2 \pmod 4$ or k is even,
2. All the elements of $S_k \subset S_{mk}$ are even if and only if $k = 1$ or m is even,
3. All the elements of $C_m \times \cdots \times C_m \subset S_{mk}$ are even if and only if m is odd.

If none of these groups includes any odd elements then the group $N_{A_{mk}}(\langle\sigma\rangle) = N_{S_{mk}}(\langle\sigma\rangle)$. If only one of these groups contains odd elements then the subgroup $N_{A_{mk}}(\langle\sigma\rangle)$ has index 2 in $N_{S_{mk}}(\langle\sigma\rangle)$ and $N_{A_{mk}}(\langle\sigma\rangle)$ can be written as a semidirect product. The case when the last two of these groups both contain odd elements never arises. If exactly two of the groups contain odd elements then elements in $N_{A_{mk}}(\langle\sigma\rangle)$ can arise as products of odd/even elements of the subgroups in two ways. The table below shows the different possible cases. If all elements of the subgroup are even we indicate this with Y; otherwise we indicate it with N.

TABLE: 5.2.7

	m	k	U_m	S_k	$(C_m)^k$	$N_{A_{mk}}(\langle\sigma\rangle)$
1	odd square	1	Y	Y	Y	$N_{S_{mk}}(\langle\sigma\rangle)$
2a	odd square	>1	Y	N	Y	$U_m \ltimes (C_m \wr A_k)$
2b	odd non-sq.	even				
3	odd non-sq.	1	N	Y	Y	$(A_m \cap U_m) \ltimes C_m$
4a	2 (mod 4)	any	Y	Y	N	$U_m \ltimes \left(S_k \ltimes (C_m \times \cdots \times C_m \times C_{\frac{m}{2}})\right)$
4b	0 (mod 4)	even				
5	odd non-sq.	odd>1	N	N	Y	The group is not a semidirect product. (See Examples 5.2.14 and 5.2.15 below.)
6	0 (mod 4)	odd	N	Y	N	

We give examples of each of these cases:

Example 5.2.8 (For Case 1)

See Example 5.2.6.

Example 5.2.9 (For Case 2a)

Let $\sigma = (1,2,3,4,5,6,7,8,9)(10,11,12,13,14,15,16,17,18)$. Here $m = 9$ and $k = 2$. Since m is an odd square all the elements of $U_9 \subset S_{18}$ are even. All the elements of $C_9 \times C_9$ are even and the centraliser is isomorphic to $C_9 \wr A_2$ with order 81. The normaliser is isomorphic to

$$U_9 \ltimes (C_9 \wr A_2) \quad \text{with order 486.}$$

Example 5.2.10 (For Case 2b)

Let $\sigma = (1,2,3)(4,5,6)(7,8,9)(10,11,12)$. Here $m = 3$ and $k = 4$. Since k is even all the elements of $U_3 \subset S_{12}$ are even. All the elements of $C_3 \times C_3 \times C_3 \times C_3$ are even and the centraliser is isomorphic to $C_3 \wr A_4$ with order 972. The normaliser

is isomorphic to

$$U_3 \ltimes (C_3 \wr A_4) \quad \text{with order } 1944.$$

Example 5.2.11 (For Case 3)

Let $\sigma = (1,2,3,4,5,6,7)$. Here $m = 7$ and $k = 1$. Since $m = 7$ is not an odd square half the elements of $U_7 \subset S_7$ are even. All the elements of $C_7 = \langle\sigma\rangle$ are even. Therefore the normaliser is isomorphic to

$$(A_7 \cap U_7) \ltimes C_7 \quad \text{with order } 21.$$

Example 5.2.12 (For Case 4a)

Let $\sigma = (1,2,3,4,5,6)(7,8,9,10,11,12)(13,14,15,16,17,18)$. Here $m = 6, k = 3$. Since $m = 6$ and $6 \equiv 2 \pmod 4$ all the elements of U_6 are even. In fact here

$$U_6 = \{\, id, (2,6)(3,5)(8,12)(9,11)(14,18)(15,17) \,\}.$$

All the elements of the copy of S_3 are even and half of the elements of $C_6 \times C_6 \times C_6$ are even. Therefore there are

$$2 \cdot 3! \cdot \frac{6^3}{2} = 1296$$

ways to get an even element. Hence $N_{A_{18}}(\langle\sigma\rangle)$ has order 1296 and is a normal subgroup of $N_{S_{18}}(\langle\sigma\rangle)$ which has order $2 \cdot 1296 = 2592$. The normaliser is isomorphic to

$$U_6 \ltimes \big(S_3 \ltimes (C_6 \times C_6 \times C_3)\big).$$

Example 5.2.13 (For Case 4b)

Let $\sigma = (1,2,3,4)(5,6,7,8)(9,10,11,12)(13,14,15,16)$. Here $m = 4$ and $k = 4$. Since k is even all the elements of $U_4 \subset S_{16}$ are even. Since m is even all the elements of $S_4 \subset S_{16}$ are even. The group consists of the elements of $C_4 \times C_4 \times C_4 \times C_4$ is isomorphic to $C_4 \times C_4 \times C_4 \times C_2$. Hence the normaliser is isomorphic to

$$U_4 \ltimes \big(S_4 \ltimes (C_4 \times C_4 \times C_4 \times C_2)\big) \quad \text{with order } 6144.$$

Example 5.2.14 (For Case 5)

Let $\sigma = (1,2,3,4,5)(6,7,8,9,10)(11,12,13,14,15)$. Here $m = 5$ and $k = 3$. Since m is not an odd square and k is odd, half the elements of $U_5 \subset S_{15}$ are even. Since m is even half the elements of $C_5 \times C_5 \times C_5$ are even and all the elements of the copy of S_3 are even. Therefore there are 2 ways to get an even element in the normaliser:

1. Even $\times$ Even $\times$ Even : 750 of them;
2. Odd $\times$ Odd $\times$ Even : 750 of them.

Notice that 750 comes from:

$$\frac{\phi(5)}{2} \cdot \frac{3!}{2} \cdot 5^3 = 750.$$

Therefore there are 1500 ways to get an even element. Hence $N_{A_{15}}(\langle\sigma\rangle)$ has order 1500 and is a normal subgroup of $N_{S_{15}}(\langle\sigma\rangle)$ which has order $2 \cdot 1500 = 3000$.

Example 5.2.15 (For Case 6)

Let $\sigma = (1,2,3,4)(5,6,7,8)(9,10,11,12)$. Here $m = 4, k = 3$. Since $m = 4 \equiv 0 \pmod 4$ half the elements of U_4 are even. In fact

$$U_4 = \{\, id, (2,4)(6,8)(10,12) \,\}.$$

All the elements of the copy of S_3 are even and half of the elements of $C_4 \times C_4 \times C_4$ are even. Now there are 2 ways to get an even element:

1. Even $\times$ Even $\times$ Even : 192 of them;
2. Odd $\times$ Even $\times$ Odd : 192 of them.

Notice that 192 comes from:

$$\frac{\phi(4)}{2} \cdot 3! \cdot \frac{4^3}{2} = 192.$$

Therefore there are 384 ways to get an even element. Hence $N_{A_{12}}(\langle\sigma\rangle)$ has order 384 and is a normal subgroup of $N_{S_{12}}(\langle\sigma\rangle)$ which has order $2 \cdot 384 = 768$.

5.3 General Case

Throughout this section, we assume that $\sigma \in S_n$ has been written as a product of disjoint regular permutations and we define the σ_{m_i}'s, the Ω_{m_i}'s and r as in Theorem 2.2.1.

Theorem 5.3.1 Suppose that σ is a permutation for which the numbers m_i are all odd squares and each $k_{m_i} = 1$. Then we have:

$$N_{S_n}(\langle\sigma\rangle) = N_{A_n}(\langle\sigma\rangle),$$

and

$$N_{A_n}(\langle\sigma\rangle) \trianglelefteq N_{A(\Omega_{m_1})}(\langle\sigma_{m_1}\rangle) \times \ldots \times N_{A(\Omega_{m_r})}(\langle\sigma_{m_r}\rangle),$$

with index

$$\frac{\phi(m_1)\phi(m_2)\ldots\phi(m_r)}{\phi\big(\mathrm{lcm}(m_1, m_2, \ldots, m_r)\big)}.$$

Proof:

Let $\alpha \in N_{S_n}(\langle\sigma\rangle)$. Since $\alpha^{-1}\sigma\alpha = \sigma^t, (t, |\sigma|) = 1$ we see that

$$\alpha = \alpha_{m_1} \ldots \alpha_{m_r} \quad \text{with} \quad \alpha_{m_i} \in N_{S(\Omega_{m_i})}(\langle\sigma_{m_i}\rangle).$$

Since m_i is an odd square with $k_{m_i} = 1$ for all i, by Corollary 5.2.5, α_{m_i} is even and therefore

$$N_{S_n}(\langle\sigma\rangle) = N_{A_n}(\langle\sigma\rangle), \quad N_{A(\Omega_{m_i})}(\langle\sigma_{m_i}\rangle) = N_{S(\Omega_{m_i})}(\langle\sigma_{m_i}\rangle) \quad \text{for every } i$$

and

$$N_{A_n}(\langle\sigma\rangle) \leqslant N_{A(\Omega_{m_1})}(\langle\sigma_{m_1}\rangle) \times \ldots \times N_{A(\Omega_{m_r})}(\langle\sigma_{m_r}\rangle).$$

Proof of normality follows from Theorem 3.4.2 and using Theorem 3.4.4 the index can be verified to be

$$\frac{\phi(m_1)\phi(m_2)\ldots\phi(m_r)}{\phi\big(\mathrm{lcm}(m_1, m_2, \ldots, m_r)\big)}.$$

□

Example 5.3.2 Let $\sigma = (1,2,\ldots,9)(10,11,\ldots,34)$, that is σ is a product of a 9-cycle and a 25-cycle. Since both 9 and 25 are odd squares and the index in the above theorem is 1, we have

$$\begin{aligned} N_{S_{34}}(\langle\sigma\rangle) = N_{A_{34}}(\langle\sigma\rangle) &\cong N_{A_9}(\langle\sigma_9\rangle) \times N_{A(\Omega_{25})}(\langle\sigma_{25}\rangle) \\ &\cong (U_9 \ltimes C_9) \times (U_{25} \ltimes C_{25}), \end{aligned}$$

with order 27000, where $\Omega_{25} = \{10,11,\ldots,34\}$.

Example 5.3.3 Let $\sigma \in S_{90}$ be a product of cycles of length 9 and 81, say

$$\sigma = \sigma_9 \cdot \sigma_{81}$$

where $\sigma_9 = (1,2,\ldots,9)$ and $\sigma_{81} = (10,11,\ldots,90)$. Let $N_i = N_{A(\Omega_i)}(\langle\sigma_i\rangle)$ for $i = 9, 81$ and let $N = N_{A_{90}}(\langle\sigma\rangle)$. We know that

$$N_{S_{90}}(\langle\sigma\rangle) = N_{A_{90}}(\langle\sigma\rangle).$$

Now, since

$$\phi(9) \cdot \phi(81) \neq \phi\big(\mathrm{lcm}(9,81)\big)$$

we have

$$N \lhd N_9 \times N_{81}$$

with index

$$\frac{\phi(9) \cdot \phi(81)}{\phi\big(\mathrm{lcm}(9,81)\big)} = 6.$$

Theorem 5.3.4 Suppose that exactly one of the m_i's (say m_1) in the above product of regular permutations is either an odd square with $k_{m_1} > 1$, or is not an odd square. Then we have:

$$N_{A_n}(\langle\sigma\rangle) \lhd N_{S_n}(\langle\sigma\rangle) \quad \text{with index 2,}$$

and

$$N_{A_n}(\langle\sigma\rangle) \trianglelefteq N_{A(\Omega_{m_1})}(\langle\sigma_{m_1}\rangle) \times \ldots \times N_{A(\Omega_{m_r})}(\langle\sigma_{m_r}\rangle)$$

with index

$$\frac{\phi(m_1)\phi(m_2)\dots\phi(m_r)}{\phi\big(\mathrm{lcm}(m_1,m_2,\dots,m_r)\big)}.$$

Proof:

Let $\alpha \in N_{A_n}(\langle\sigma\rangle)$. Since $\alpha^{-1}\sigma\alpha = \sigma^t$ with $(t,|\sigma|)=1$, then

$$\alpha = \alpha_{m_1}\dots\alpha_{m_r} \quad \text{where} \quad {\alpha_{m_i}}^{-1}\sigma_{m_i}\alpha_{m_i} = {\sigma_{m_i}}^t.$$

Since $m_2, m_3, \dots, m_r$ are all odd squares with $k_{m_2} = k_{m_3} = \dots = k_{m_r} = 1$ we see that $\alpha_{m_2}, \dots, \alpha_{m_r}$ must all be even. Since α is even α_{m_1} must be even too. Therefore

$$N_{A_n}\big(\langle\sigma\rangle\big) \leqslant N_{A(\Omega_{m_1})}\big(\langle\sigma_{m_1}\rangle\big) \times \dots \times N_{A(\Omega_{m_r})}\big(\langle\sigma_{m_r}\rangle\big).$$

In order to prove the normality we let

$$h_i \in N_{A(\Omega_{m_i})}\big(\langle\sigma_{m_i}\rangle\big) \text{ with } {h_i}^{-1}\sigma_{m_i}h_i = {\sigma_{m_i}}^{t_i}, \text{ where } (t_i,m_i)=1.$$

Let $\overline{t_i}$ represent the inverse of t_i in U_{m_i} as in Proposition 3.2.4. Let $n \in N_{A_n}\big(\langle\sigma\rangle\big)$ with $n^{-1}\sigma n = \sigma^t$, and let $h = h_1h_2\dots h_r$. We need to show that $h^{-1}nh \in N_{A_n}\big(\langle\sigma\rangle\big)$.

$$\begin{aligned}
(h^{-1}nh)^{-1}\sigma(h^{-1}nh) &= h^{-1}n^{-1}h\sigma h^{-1}nh \\
&= h^{-1}n^{-1}h_1\dots h_r\sigma {h_r}^{-1}\dots {h_1}^{-1}nh \\
&= h^{-1}n^{-1}{\sigma_{m_1}}^{\overline{t_1}}\dots {\sigma_{m_r}}^{\overline{t_r}}nh \\
&= h^{-1}{\sigma_{m_1}}^{\overline{t_1}t}\dots {\sigma_{m_r}}^{\overline{t_r}t}h \\
&= {\sigma_{m_1}}^{\overline{t_1}tt_1}\dots {\sigma_{m_r}}^{\overline{t_r}tt_r} \\
&= {\sigma_{m_1}}^{t}\dots {\sigma_{m_r}}^{t} \\
&= \sigma^t.
\end{aligned}$$

Since m_1 is either an odd square with $k_{m_1} > 1$, or is not an odd square, $N_{S(\Omega_1)}\big(\langle\sigma_{m_1}\rangle\big)$ will include odd elements, so we have

$$N_{A_n}\big(\langle\sigma\rangle\big) \lhd N_{S_n}\big(\langle\sigma\rangle\big) \quad \text{with index 2.}$$

By Theorem 3.4.1 and Theorem 2.2.1 we have the following:

$$\begin{aligned}\left|N_{A_n}(\langle\sigma\rangle)\right| &= \tfrac{1}{2}\left|N_{S_n}(\langle\sigma\rangle)\right| \\ &= \tfrac{1}{2}\left|C_{S_n}(\sigma)\right| \cdot \left|U_{|\sigma|}\right| \\ &= \tfrac{1}{2}\, k_{m_1}!\, {m_1}^{k_{m_1}} \ldots k_{m_r}!\, {m_r}^{k_{m_r}}\ \phi\big(\mathrm{lcm}(m_1, \ldots, m_k)\big).\end{aligned}$$

To find the order of the direct product we have

$$\left|N_{A(\Omega_{m_i})}(\langle\sigma_{m_i}\rangle)\right| = \begin{cases} \frac{1}{2}\phi(m_i)\, k_{m_i}!\, {m_i}^{k_{m_i}} & \text{if } i = 1, \\ \\ \phi(m_i)\, k_{m_i}!\, {m_i}^{k_{m_i}} & \text{otherwise.} \end{cases}$$

So the order of the direct product is

$$\frac{1}{2}\ \phi(m_1)\, k_{m_1}!\, m_1^{k_{m_1}} \cdots \phi(m_r)\, k_{m_r}!\, m_r^{k_{m_r}}.$$

Therefore the required index is:

$$\frac{\phi(m_1) \ldots \phi(m_r)}{\phi\big(\mathrm{lcm}(m_1, \ldots, m_r)\big)}.$$

□

Example 5.3.5 Let $\sigma = \sigma_6 \cdot \sigma_9 \cdot \sigma_{81}$ where

$$\begin{aligned}\sigma_6 &= (1, 2, \ldots, 6)(7, 8, \ldots, 12), \\ \sigma_9 &= (13, 14, \ldots, 21), \\ \sigma_{81} &= (22, 23, \ldots, 102).\end{aligned}$$

Now we have $|\sigma| = 162$. Let N_i be the normaliser of subgroup generated by σ_i in $A(\Omega_i)$ for $i = 6, 9, 81$. Now $\alpha \in N_{A_{102}}\big(\langle\sigma\rangle\big)$ conjugates σ into σ^t with $(t, 162) = 1$. That is, $\alpha = \alpha_6 \cdot \alpha_9 \cdot \alpha_{81}$ where $\alpha_6, \alpha_9, \alpha_{81}$ conjugate $\sigma_6, \sigma_9, \sigma_{81}$ into ${\sigma_6}^t, {\sigma_9}^t, {\sigma_{81}}^t$ respectively. Since 9 and 81 are odd squares and σ_9 and σ_{81} consist of only one cycle, α_9 and α_{81} must be even. This means that α_6 must be even too. Therefore there is only one way to get an even element. That is

$$\text{Even} \times \text{Even} \times \text{Even}.$$

Therefore

$$N_{A_{102}}(\langle\sigma\rangle) \leqslant N_6 \times N_9 \times N_{81}.$$

Normality can be proven easily. The size of $N_{A_{102}}(\langle\sigma\rangle)$ is:

$$\phi(162) \cdot \frac{2! \cdot 6^2}{2} \cdot 9 \cdot 81 = 1417176.$$

The index of $N_{A_{102}}(\langle\sigma\rangle)$ in $N_6 \times N_9 \times N_{81}$ is

$$\frac{\phi(6) \cdot \phi(9) \cdot \phi(81)}{\phi(162)} = 12.$$

Since $N_{S_{12}}(\langle\sigma_6\rangle)$ will include odd elements we have:

$$N_{A_{102}}(\langle\sigma\rangle) \lhd N_{S_{102}}(\langle\sigma\rangle) \quad \text{with index 2.}$$

Example 5.3.6 Let $\sigma = \sigma_{28} \cdot \sigma_9 \cdot \sigma_{25}$ where

$$\sigma_{28} = (1, 2, \ldots, 28),$$
$$\sigma_9 = (29, 30, \ldots, 37),$$
$$\sigma_{25} = (38, 39, \ldots, 62).$$

This example is very similar to the previous one but since here we have that $28, 9, 25$ lead to an index of 1 in the Theorem 5.3.4, we have

$$N_{A_{62}}(\langle\sigma\rangle) \cong N_{28} \times N_9 \times N_{25}.$$

Theorem 5.3.7 Suppose that in the above product of regular permutations the number of the m_i's which are not odd squares or which are odd squares with $k_{m_i} > 1$ is two or more. Then we have:

$$N_{A_n}(\langle\sigma\rangle) \lhd N_{S_n}(\langle\sigma\rangle) \quad \text{with index 2.}$$

Here we have two cases:

If the m_i's do not satisfy

$$\phi(m_1)\phi(m_2)\ldots\phi(m_r) = \phi(\text{lcm}(m_1, m_2, \ldots, m_r)) \tag{5.1}$$

then neither the normaliser of $\langle\sigma\rangle$ nor the direct product of normalisers of subgroups generated by σ_{m_i}'s is a subgroup of the other.

If the m_i's satisfy (5.1) then let

$$u = (\text{number of } i\text{'s such that } m_i \text{ is not an odd square}$$
$$\text{or } m_i \text{ is an odd square with } k_{m_i} > 1) - 1.$$

Then we have

$$N_{A(\Omega_{m_1})}(\langle\sigma_{m_1}\rangle) \times \ldots \times N_{A(\Omega_{m_r})}(\langle\sigma_{m_r}\rangle) \lhd N_{A_n}(\langle\sigma\rangle)$$

with index 2^u.

Proof:

Since we have 2 or more m_i's which are not odd squares or which are odd squares with $k_{m_i} > 1$, let m_1 and m_2 be such numbers. First of all, since $N_{S(\Omega_{m_1})}(\langle\sigma_{m_1}\rangle)$ will include odd elements we have:

$$N_{A_n}(\langle\sigma\rangle) \lhd N_{S_n}(\langle\sigma\rangle) \quad \text{with index 2.}$$

Let $\alpha \in N_{A_n}(\langle\sigma\rangle)$ conjugate σ into σ^t with $(t, |\sigma|) = 1$. Then $\alpha = \alpha_{m_1} \ldots \alpha_{m_r}$ where α_{m_i} conjugates σ_{m_i} into ${\sigma_{m_i}}^t$. Since α_{m_1} and α_{m_2} can both be odd we see that

$$N_{A_n}(\langle\sigma\rangle) \not\leq N_{A(\Omega_{m_1})}(\langle\sigma_{m_1}\rangle) \times \ldots \times N_{A(\Omega_{m_r})}(\langle\sigma_{m_r}\rangle).$$

Now let $\alpha_{m_i} \in N_{A(\Omega_{m_i})}(\langle\sigma_{m_i}\rangle)$ conjugate σ_{m_i} into ${\sigma_{m_i}}^{t_i}$ with t_i coprime to m_i. Their product $\alpha_{m_1} \ldots \alpha_{m_r}$ conjugates σ into a power of σ coprime to m if and only if the m_i's satisfy (5.1). Therefore

$$N_{A(\Omega_{m_1})}(\langle\sigma_{m_1}\rangle) \times \ldots \times N_{A(\Omega_{m_r})}(\langle\sigma_{m_r}\rangle) \lhd N_{A_n}(\langle\sigma\rangle)$$

if and only if m_i's satisfy (5.1).

The normality can be proven easily. Now assume that m_i's satisfy (5.1), then

$$\left|N_{A(\Omega_{m_j})}(\langle\sigma_{m_j}\rangle)\right| = \begin{cases} \phi(m_j)\, k_{m_j}!\, {m_j}^{k_{m_j}} & \text{if } m_j \text{ is an odd square and } k_{m_j}=1, \\ \frac{1}{2}\phi(m_j)\, k_{m_j}!\, {m_j}^{k_{m_j}} & \text{otherwise} \end{cases}$$

and

$$\left|N_{A_n}(\langle\sigma\rangle)\right| = \frac{1}{2}\cdot\phi\big(\mathrm{lcm}(m_1,\ldots,m_r)\big)\cdot k_{m_1}!{m_1}^{k_{m_1}}\cdot\ldots\cdot k_{m_r}!{m_r}^{k_{m_r}}.$$

The index, therefore, is:

$$\frac{2^{r-\bar{r}}}{2} = 2^{r-\bar{r}-1}$$

where $\bar{r}$ is the number of m_i's which are odd squares with $k_{m_i}=1$, so $u = r-\bar{r}-1$. □

Remark 5.3.8 By the proof of Corollary 3.4.6 the identity in (5.1) in the statement of Theorem 5.3.7 is satisfied if and only if the odd parts of the m_i's are pairwise coprime and at most one of the m_i's is divisible by 4.

Example 5.3.9 Let $\sigma = \sigma_4\cdot\sigma_{12}\cdot\sigma_{20}$ where

$$\sigma_4 = (1,2,3,4),$$
$$\sigma_{12} = (5,6,\ldots,16),$$
$$\sigma_{20} = (17,18,\ldots,36).$$

Now $|\sigma| = 60 = \mathrm{lcm}(4,12,20)$. Let $N = N_{A_{36}}\big(\langle\sigma\rangle\big)$ and

$$N_i = N_{A(\Omega_i)}\big(\langle\sigma_i\rangle\big) \text{ for } i = 4,12,20.$$

Now, an element, say α, of N conjugates σ into σ^t where $(t,60)=1$. That is, $\alpha = \alpha_4\cdot\alpha_{12}\cdot\alpha_{20}$ with α_i conjugating σ_i into ${\sigma_i}^t$ for $i = 4,12,20$. We notice that, for example, α_4 and α_{12} can be both odd. Therefore

$$N \not\leqslant N_4\times N_{12}\times N_{20}.$$

Now assume that $\alpha_4 \in N_4$ conjugates σ_4 into ${\sigma_4}^3$, $\alpha_{12} \in N_{12}$ conjugates σ_{12} into ${\sigma_{12}}^5$, $\alpha_{20} \in N_{20}$ conjugates σ_{20} into ${\sigma_{20}}^7$, Then $\sigma_4 \cdot \sigma_{12} \cdot \sigma_{20}$ conjugates σ into ${\sigma_4}^3 \cdot {\sigma_{12}}^5 \cdot {\sigma_{20}}^7$ which is not a power of σ. Therefore $N_4 \times N_{12} \times N_{20}$ cannot be a subgroup of N. Notice that one can always find such numbers if the m_i's do not satisfy (5.1).

Example 5.3.10 Let $\sigma = \sigma_4 \cdot \sigma_7 \cdot \sigma_9 \cdot \sigma_{10}$ where

$$\sigma_4 = (1,2,3,4)(5,6,7,8),$$
$$\sigma_7 = (9,10,11,12,13,14,15),$$
$$\sigma_9 = (16,17,18,19,20,21,22,23,24),$$
$$\sigma_{10} = (25,26,27,28,29,30,31,32,33,34).$$

Now $|\sigma| = 1260 = \text{lcm}(4,7,9,10)$. Let $N = N_{A_{34}}(\langle\sigma\rangle)$ and

$$N_i = N_{A(\Omega_i)}(\langle\sigma_i\rangle) \text{ for } i = 4,7,9,10.$$

Now, an element, say α, of N conjugates σ into σ^t where $(t,1260) = 1$. That is, $\alpha = \alpha_4 \cdot \alpha_7 \cdot \alpha_9 \cdot \alpha_{10}$ with α_i conjugating σ_i into ${\sigma_i}^t$ for $i = 4,7,9,10$. We notice that, for example, α_4 and α_7 can be both odd. Therefore N cannot be a subgroup of $N_4 \times N_7 \times N_9 \times N_{10}$.

Now assume that $\alpha_i \in N_i$ conjugates σ_i into ${\sigma_i}^{t_i}$ for $i = 4,7,9,10$ where $(t_i, i) = 1$. Then $\alpha_4 \cdot \alpha_7 \cdot \alpha_9 \cdot \alpha_{10}$ conjugates σ into ${\sigma_4}^{t_4} \cdot {\sigma_7}^{t_7} \cdot {\sigma_9}^{t_9} \cdot {\sigma_{10}}^{t_{10}}$ which is always a coprime power of σ since $4,7,9,10$ satisfy (5.1). Or in other words the map

$$f : U_{1260} \longrightarrow U_4 \times U_7 \times U_9 \times U_{10}$$

defined by

$$f(x) = (x \bmod 4, x \bmod 7, x \bmod 9, x \bmod 10)$$

is an isomorphism. Therefore

$$N_4 \times N_7 \times N_9 \times N_{10} \lhd N$$

To find the index we have:

$$|N_i| = \phi(i) \cdot \frac{k_i! \cdot i^{k_i}}{2} \text{ for } i = 4, 7, 10$$

while

$$|N_9| = \phi(9) \cdot 9 \quad \text{(since 9 is an odd square and } k_9 = 1.\text{)}$$

So the index is

$$\frac{\frac{1}{2} \cdot \phi(1260) \cdot 2! \cdot 4^2 \cdot 7 \cdot 9 \cdot 10}{\frac{\phi(4) \cdot 2! \cdot 4^2}{2} \cdot \frac{\phi(7) \cdot 7}{2} \cdot \phi(9) \cdot 9 \cdot \frac{\phi(10) \cdot 10}{2}} = 4.$$

□

5.4 A Subgroup Lattice Diagram

In this section we summarise some of main results we obtained. The lattice diagram in Figure 5.1 shows the relations among the groups we have studied in this work.

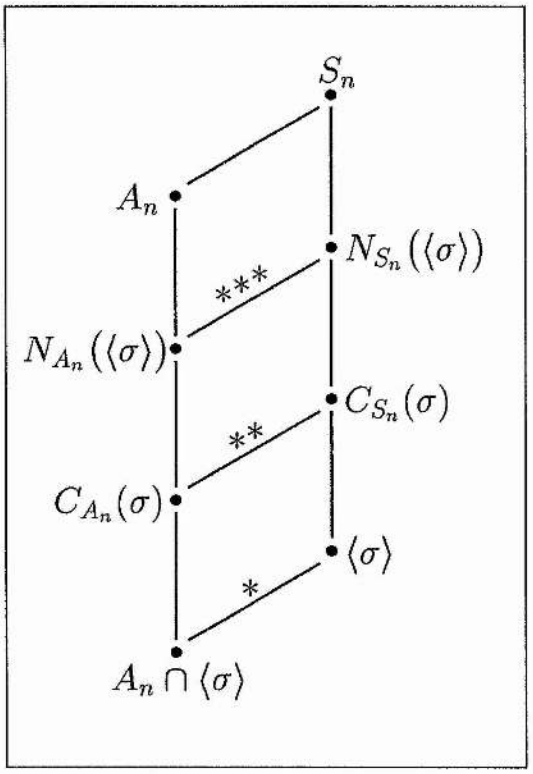


Figure 5.1: Subgroup lattice diagram of centralisers and normalisers

Now let σ be an element of S_n with no fixed point. Let σ be a product of k_1 disjoint m_1-cycles, ... , k_r disjoint m_r-cycles. Then in the subgroup lattice diagram:

1. $*$ is an isomorphism if and only if σ is an even permutation,

2. $**$ is an isomorphism if and only if $k_i = 1$ and m_i is odd for every i (see the

proof of Theorem 4.3.2),

3. $***$ is an isomorphism if and only if $k_i = 1$ and m_i is an odd square for every i; otherwise the subgroup has index 2 (by Theorems 5.3.1, 5.3.4, 5.3.7).

We also examined the relationship between the centraliser/normaliser of σ and the direct product of the centralisers/normaliser of regular parts in S_n and A_n. We also have given the index of the subgroup for each case. The following list tells you where you can find them:

1. For centralisers in S_n see Theorem 2.2.1.
2. For normalisers in S_n see Theorems 3.4.2, 3.4.4.
3. For centralisers in A_n see Theorem 4.3.2.
4. For normalisers in A_n see Theorems 5.3.1, 5.3.4, 5.3.7.

Chapter 6

Developing the GAP Package

6.1 Introduction

In this chapter we will give some functions and programs that we used in this work. The GAP language is described clearly in [18], which we refer as The GAP Manual. These functions and programs will be useful for someone who is interested in computational group theory, especially in permutation groups. Some other functions and programs can be found in [1], but some of those functions come as standard in the new versions of GAP. For a complete list of functions see The GAP Manual. The functions we give here are written in GAP version 3.4.4.

On starting GAP one sees the following: (see Figure 6.1)

```
      ########             Lehrstuhl D fuer Mathematik
    ###    ####            RWTH Aachen
   ##         ##
  ##           #              #######            #########
 ##                         #       ##         ## #     ##
 ##           #            #        ##            #      ##
 ####        ##            ##       #             #      ##
  #####     ###            ##       ##            ##    ##
    ######### #             #########             #######
             #                                     #
            ##             Version 3              #
           ###             Release 4.4            #
          ## #             18 Apr 97              #
         ##  #
        ##   #  Alice Niemeyer, Werner Nickel,  Martin Schoenert
       ##    #  Johannes Meier, Alex Wegner,    Thomas Bischops
      ##     #  Frank Celler,   Juergen Mnich,  Udo Polis
      ###   ##  Thomas Breuer,  Goetz Pfeiffer, Hans U. Besche
       ######   Volkmar Felsch, Heiko Theissen, Alexander Hulpke
                Ansgar Kaup,    Akos Seress,    Erzsebet Horvath
                Bettina Eick
                For help enter: ?<return>
gap>
```

Figure 6.1: The GAP banner.

This GAP banner is just a greeting and it is not important in the program. It is followed by the GAP prompt: "**gap>**" and it indicates that GAP expects you to enter some command. After each computation the prompt appears again. If this prompt did not appear it would mean that either GAP was still computing or an error had occured. The word "**quit;**" after the prompt with the <newline> or <return> key will exit you from GAP and take you back from where you started. To compute an expression in GAP you write it after the prompt and then end it with a semi-colon. On pressing <return> GAP will then attempt to evaluate the expression.

The operations in GAP depend on the type of input. For example, to calculate the product of integers 2 and 3, we type $2*3$; after the prompt and the press the <return> key to get 6. i.e.,

```
gap> 2*3;
6
gap>
```

Throughout this work, the output that GAP returns is printed in `typewriter` font and the input given to GAP by the user is printed in **bold-typewriter** font.

Permutations in GAP operate on positive integers, and they are entered and displayed in cycle notation.

```
gap> (1,2,3);
(1,2,3)
gap> (1,2,3) * (2,3,4);
(1,3)(2,4)
gap>
```

Now we give the following example:

Example 6.1.1 In this example we compute the centraliser of σ and normaliser of $\langle\sigma\rangle$ in S_6, where $\sigma = (1,2,3)(4,5,6)$. We use GAP to calculate the orders of S_6, the centraliser and the normaliser.

```
gap> s6 := Group((1,2,3,4,5,6),(1,2));
Group( (1,2,3,4,5,6), (1,2) )
gap> sigma := (1,2,3)(4,5,6);
(1,2,3)(4,5,6)
gap> h := Subgroup(s6,[sigma]);
Subgroup( Group( (1,2,3,4,5,6), (1,2) ), [ (1,2,3)(4,5,6) ] )
gap> Size(h);
3
gap> c := Centralizer(s6,sigma);
```

```
Subgroup( Group( (1,2,3,4,5,6), (1,2) ),
[ (1,2,3)(4,5,6), (4,5,6), (1,4)(2,5)(3,6) ] )
gap> n := Normalizer(s6,h);
Subgroup( Group( (1,2,3,4,5,6), (1,2) ),
[ (1,2,3)(4,5,6), (4,5,6), (2,3)(5,6), (1,4)(2,5)(3,6) ] )
gap> Size(s6); Size(c); Size(n);
720
18
36
gap> quit;
```

6.2 Functions

Function 6.2.1 The function `cycle(n)` returns $(1, 2, \ldots, n)$, while the second form `cycle(n,b)` returns $(b, b+1, \ldots, b+n-1)$, i.e. the cycle of length n with first symbol b. Remember to use it with lowercase c because `Cycle` is a predefined function in GAP.

```
#-------------------------------------------------------------
cycle := function(arg)
local n,b,p,i;
if Length(arg)=1 then
   if IsInt(arg[1]) then
        if arg[1]< 1 then
          Error("argument must be an integer > 0");
        fi;
   else
      Error("argument must be an integer");
   fi;
fi;
if Length(arg)=2 then
   if IsInt(arg[1]) and IsInt(arg[2]) then
       if arg[1]<1 or arg[2]<1 then
          Error("arguments must me > 0");
       fi;
   else
      Error("arguments must be integers");
   fi;
fi;
n:=arg[1];
```

```
if Length(arg)=2 then b:=arg[2]; else b:=1; fi;
p:=();
for i in [b+1..b+n-1] do p:=p*(b,i); od;
return p;
end;
#-------------------------------------------------------------
```

Example 6.2.2

```
gap> cycle(6);
(1,2,3,4,5,6)
gap> cycle(5,3);
(3,4,5,6,7)
gap>
```

Function 6.2.3 The function `MovedPoints(p)` returns the list of points which are moved by `p` in an increasing order.

```
#-------------------------------------------------------------
MovedPoints := function(p)
local i,m,l;
if not IsPerm(p) then
   Error("argument must be a permutation");
fi;
l:=[];
if p=() then return []; fi;
m:=LargestMovedPointPerm(p);
for i in [1..m] do
 if i^p<>i then Add(l,i); fi;
od;
return l;
```

```
end;
#-------------------------------------------------------------
```

Example 6.2.4

```
gap> MovedPoints((2,3,5)(1,6));
[ 1, 2, 3, 5, 6 ]
gap> MovedPoints(());
[ ]
gap>
```

Function 6.2.5 The function `IsCycle(p)` returns true if the permutation `p` is a cycle, returns false otherwise. This function uses GAP's `Cycle(p,s)` function which returns the orbit of the point `s` in `p`.

```
#-------------------------------------------------------------
IsCycle := function(p)
local mp,s  ;
if not IsPerm(p) then
  Error("argument must be a permutation");
fi;
if p=() then return true; fi;
mp:=MovedPoints(p);
s:=SmallestMovedPointPerm(p);
if Length(Cycle(p,s))=Length(mp) then
   return true;
else
   return false;
fi;
end;
#-------------------------------------------------------------
```

Example 6.2.6

```
gap> IsCycle((2,3,5)(1,6));
false
gap> IsCycle((5,6,7)); IsCycle(());
true
true
gap>
```

Function 6.2.7 The function `RegularPerm(m,k)` produces a regular permutation which is a product of `k` disjoint `m`-cycles. This function is also very useful to produce cycles since `RegularPerm(m,1)` produces $(1, 2, \ldots, m)$.

```
#-------------------------------------------------------------
RegularPerm := function(m,k)
local i,j,x;
if not IsInt(m) or not IsInt(k) then
  Error("arguments must be positive integers");
fi;
if m<0 or k<0 then
   Error("arguments must be positive integers");
fi;
x:=();
for i in [0..k-1] do
    for j in [1..m-1] do
       x:= x * (m*i+1,m*i+1+j);
    od;
od;
return x;
end;
```

```
#-------------------------------------------------------------
```

Example 6.2.8

```
gap> RegularPerm(3,4);
( 1, 2, 3)( 4, 5, 6)( 7, 8, 9)(10,11,12)
gap>
```

Function 6.2.9 The function `ListToCycle(l)` produces a cycle, say x, from list `l` of integers, where x maps `l[i]` into `l[i+1]`. In other words, x is the cycle which is obtained from `l` by replacing square brackets with parentheses.

```
#-------------------------------------------------------------
ListToCycle := function(l)
local p,i,fl;
if not IsList(l) then
  Error("argument must be a list");
fi;
fl:=Flat(l);
if l<>fl or Length(Set(l))<>Length(fl) then
  Error("list must not have holes or repeated elements");
fi;
p:=();
for i in [2..Length(l)] do
 p:=p*(l[1],l[i]);
od;
return p;
end;
#-------------------------------------------------------------
```

Example 6.2.10

```
gap> ListToCycle([1,2,3,5,7,6]);
(1,2,3,5,7,6)
gap> ListToCycle([2,3,4,1]);
(1,2,3,4)
gap>
```

Function 6.2.11 The function `CycleToList(c)` produces the list `l` of integers in `c` starting from the minimum symbol and then the image of it and so on.

```
#-------------------------------------------------------------------
CycleToList := function(c)
local p,m,l,pos;
if not IsCycle(c) then
   Error("argument must be a cycle");
fi;
if c=() then return []; fi;
m:=SmallestMovedPointPerm(c);
l:=[m];
pos:=1;
repeat
  p:=l[pos]^c;
  pos:=pos+1;
  l[pos]:=p;
until p^c=m;
return l;
end;
#-------------------------------------------------------------------
```

Example 6.2.12

```
gap> CycleToList((2,1,3,5,7,6));
```

```
[ 1, 3, 5, 7, 6, 2 ]
gap>
```

Function 6.2.13 The function `S(n)` returns the symmetric group S_n if `n` is an integer, or returns the symmetric group on `n` when `n` is a list of positive integers. GAP has already `SymmetricGroup(n)` function for an integer `n` which produces S_n.

```
#-------------------------------------------------------------------
S := function(arg)
local n,l,fl;
if IsInt(arg[1]) then
   n:=arg[1];
   return(SymmetricGroup(n));
elif IsList(arg[1]) then
     l:=arg[1];
     fl:=Flat(l);
       if l<>fl or Length(Set(fl))<>Length(fl) then
       Error("the list must not contain holes
               or repeated elements");
       fi;
     n:=Length(l);
     if n=1 then
         return Group(());
     else
        return Group( ListToCycle(l),(l[1],l[2]));
     fi;
else
    Error("argument must be an integer > 1
```

```
            or a list of positive integers");
fi;
end;
#-------------------------------------------------------------
```

Example 6.2.14

```
gap> S(6);
Group( (1,6), (2,6), (3,6), (4,6), (5,6) )
gap> S([1,2,4,5,6,8]);
Group( (1,2,4,5,6,8), (1,2) )
gap>
```

Function 6.2.15 The function `A(n)` returns the alternating group A_n if `n` is an integer, or returns the alternating group on `n` when `n` is a list of positive integers.

```
#-------------------------------------------------------------
A := function(arg)
local n,l,fl;
if IsInt(arg[1]) then
   n:=arg[1];
     if n<2 then
        Error("argument must be an integer > 1");
     elif n=2 then
          return Group(());
     elif n mod 2 = 0 then
          return Group( cycle(n-1),(1,2,n));
     else
          return Group( cycle(n),(1,2,n));
     fi;
elif IsList(arg[1]) then
```

```
    l:=arg[1];
    fl:=Flat(l);
      if l<>fl or Length(Set(fl))<>Length(fl) then
      Error("the list must not contain holes
              or repeated elements");
      fi;
    n:=Length(l);
    if n=2 then
        return Group(());
    elif n mod 2 = 0 then
       return
       Group(ListToCycle(l)*(l[1],l[n]),(l[1],l[2],l[n]));
    else
       return Group( ListToCycle(l),(l[1],l[2],l[n]));
    fi;
else
   Error("argument must be an integer > 1
          or a list of positive integers");
fi;
end;
#-------------------------------------------------------------
```

Example 6.2.16

```
gap> A(5);
Group( (1,2,3,4,5), (1,2,5) )
gap> A([2,4,5,6,8,9]);
Group( (2,4,5,6,8), (2,4,9) )
gap>
```

Function 6.2.17 The function `CoprimeList(n)` returns the list of positive in-

tegers which are coprime to n and less than n, where n is a positive integer.

```
#-------------------------------------------------------------
CoprimeList := function (n)
local i,l;

if not IsInt(n) then
   Error("argument must be an integer > 0");
fi;
if n<1 then
   Error("argument must be an integer > 0");
fi;
l:=[];
for i in [1..n-1] do
  if Gcd(i,n)=1 then Add(l,i); fi;
 od;
return l;
end;
#-------------------------------------------------------------
```

Example 6.2.18

```
gap> CoprimeList(18);
[ 1, 5, 7, 11, 13, 17 ]
gap>
```

Function 6.2.19 The function `Deleted(l,x)` returns a list with `x` deleted from `l`. It also deletes holes, but it does not change the value of `l`.

```
#-------------------------------------------------------------
Deleted := function(l,x)
```

```
if not IsList(l) then
   Error("first argument must be a list");
fi;
return Filtered(l,y->(y<>x));
end;
#-------------------------------------------------------------
```

Example 6.2.20

```
gap> lst:=[1,2,3,,,5,6,2];
[ 1, 2, 3,,, 5, 6, 2 ]
gap> d:=Deleted(lst,2);
[ 1, 3, 5, 6 ]
gap> lst;
[ 1, 2, 3,,, 5, 6, 2 ]
gap>
```

Function 6.2.21 The function `CyclesOfPerm(p)` returns a list of cycles in `p`

```
#-------------------------------------------------------------
CyclesOfPerm := function(p)
local l,mp,x,keepx,subl;

if not IsPerm(p) then
   Error("argument must be a permutation");
fi;
if p=() then return []; fi;
l:=[];
mp:=MovedPoints(p);
repeat
   x:=mp[1]; mp:=Deleted(mp,x);
```

```
   keepx:=x;
   subl:=[x];
    repeat
      x:=x^p;
      Add(subl,x); mp:=Deleted(mp,x);
    until x^p=keepx;
   Add(l,ListToCycle(subl));
until mp=[];
return l;
end;
#-------------------------------------------------------------------
```

Example 6.2.22

```
gap> CyclesOfPerm((4,5)(6,7,1)(8,9,10,2));
[ (1,6,7), ( 2, 8, 9,10), (4,5) ]
gap>
```

Function 6.2.23 The function `ShifList(l,n)` returns a list which is constructed by shifting (with wraparound) the elements of `l` `n` times forward. When `n` is a negative integer the list will be shifted backwards. This function uses GAP's `Permuted(list,perm)` function which permutes `list` according to the given permutation `perm`.

```
#-------------------------------------------------------------------
ShiftList := function(l,n)

if not IsList(l) then
Error("first argument must be a list");
fi;
if not IsInt(n) then
```

```
Error("second argument must be an integer");
fi;
return Permuted(l,cycle(Length(l))^n);
end;
#----------------------------------------------------------------
```

Example 6.2.24

```
gap> ShiftList([1,2,3,4,5],1);
[ 5, 1, 2, 3, 4 ]
gap> ShiftList([1,2,3,4,5],-202);
[ 3, 4, 5, 1, 2 ]
gap>
```

Function 6.2.25 The function `ConjugatesTwoCycles(c1,c2,x)` returns a permutation which conjugates `c1` into `c2` and fixes the symbol `x`. Here, `c1` and `c2` must be two cycles acting on the same set of symbols and `x` must be a symbol which occurs in `c1`.

```
#----------------------------------------------------------------
ConjugatesTwoCycles := function(c1,c2,x)

local l1,l2;
if (not IsCycle(c1)) or
   (not IsCycle(c2)) or
   (not IsInt(x)) then
Error("usage: ConjugatesTwoCycles(<cycle>,<cycle>,<int>)");
fi;
l1:=CycleToList(c1);
l2:=CycleToList(c2);
if Set(l1)<>Set(l2) then
```

```
  Error("cycles must act on the same set of symbols");
fi;
if not (x in l1) then
  Error(x," must be a symbol in ",c1,"\n");
fi;
while Position(l1,x)<>Position(l2,x) do
 l2:=ShiftList(l2,1);
od;
return MappingPermListList(l1,l2);
end;
#-------------------------------------------------------------
```

Example 6.2.26

```
gap> sigma:=(1,2,3,4,5,6,7,8);
(1,2,3,4,5,6,7,8)
gap> ConjugatesTwoCycles(sigma,sigma^3,1);
(2,4)(3,7)(6,8)
gap>
```

Function 6.2.27 The function `Commute(h,k)` returns true if the elements of the group `h` commute with the elements of the group `k`, returns false otherwise.

```
#-------------------------------------------------------------
Commute := function(h,k)
local a,b,genh,genk;
if (not IsGroup(h)) or (not IsGroup(k)) then
   Error("arguments must be groups");
fi;
genh:=h.generators;
genk:=k.generators;
```

```
for a in genh do
    for b in genk do
      if a*b<>b*a then return false; fi;
    od;
od;
return true;
end;
#-------------------------------------------------------------
```

Example 6.2.28

```
gap> Commute(A(4),S(3));
false
gap> Commute(A(3),S([4,5,6]));
true
gap>
```

Function 6.2.29 In GAP a "set" is an ordered list with no holes. The function `SetProduct(h,k)` returns the set product of two permutation groups. If `h` is a complete set of elements of a group `g` then the boolean expression `h=g` returns `true` in GAP. Therefore this function can be used to determine whether a group is equal to the set product of its two subgroups.

```
#-------------------------------------------------------------
SetProduct := function(h,k)
local s,a,elh;
if not IsPermGroup(h) or not IsPermGroup(k) then
   Error("arguments must be permutation groups");
fi;
s:=[];
elh := Elements(h);
```

```
for a in elh do
    UniteSet(s,Set(Elements(a*k)));
od;
return s;
end;
#-------------------------------------------------------------------
```

Example 6.2.30

```
gap> h:=Group((1,2,3)); k:=Group((4,5,6));
Group( (1,2,3) )
Group( (4,5,6) )
gap> g:=Group((1,2,3),(4,5,6));
Group( (1,2,3), (4,5,6) )
gap> g=SetProduct(h,k);
true
gap>
```

Function 6.2.31 The function `IsInternalDirectProduct(g,h,k)` returns true if `g` is the direct product of its subgroups `h` and `k`, false otherwise.

```
#-------------------------------------------------------------------
IsInternalDirectProduct := function(g,h,k)
if not IsPermGroup(g) or
   not IsPermGroup(h) or
   not IsPermGroup(k)  then
    Error("arguments must be permutation groups");
fi;
if Size(g)<>Size(h)*Size(k) then
  return false;
fi;
```

```
if not IsNormal(g,h) or not IsNormal(g,k) then
  return false;
fi;
if Length(Elements(Intersection(h,k))) > 1  then
 return false;
fi;
if Subgroup(g,Union(h.generators,k.generators))=g then
   return true;
else
   return false;
fi;
end;
#-------------------------------------------------------------
```

Example 6.2.32

```
gap> g:=Group((1,2,3),(4,5,6));
Group( (1,2,3), (4,5,6) )
gap> h:=Subgroup(g,[(1,2,3)]);
Subgroup( Group( (1,2,3), (4,5,6) ), [ (1,2,3) ] )
gap> k:=Subgroup(g,[(4,5,6)]);
Subgroup( Group( (1,2,3), (4,5,6) ), [ (4,5,6) ] )
gap> IsInternalDirectProduct(g,h,k);
true
gap>
```

Function 6.2.33 The function `IsSemiDirectProduct(g,n,k)` returns true if g is the semidirect direct product of its normal subgroup n by k, false otherwise.

```
#-------------------------------------------------------------
IsSemiDirectProduct := function(g,n,k)
```

```
if not IsPermGroup(g) or
   not IsPermGroup(n) or
   not IsPermGroup(k)  then
    Error("arguments must be permutation groups");
fi;
if Size(g)<>Size(n)*Size(k) then
  return false;
fi;
if not IsNormal(g,n) or not IsSubgroup(g,k) then
  return false;
fi;
if Length(Elements(Intersection(n,k)))>1  then
 return false;
fi;
if Subgroup(g,Union(n.generators,k.generators))=g then
    return true;
else
    return false;
fi;
end;
#-------------------------------------------------------------
```

Example 6.2.34

```
gap> g:=Group((1,2,3),(1,4)(2,5)(3,6)); g.name:="G";
Group( (1,2,3), (1,4)(2,5)(3,6) )
"G"
gap> n:=Subgroup(g,[(1,2,3),(4,5,6)]);
Subgroup( G, [ (1,2,3), (4,5,6) ] )
gap> k:=Subgroup(g,[(1,4)(2,5)(3,6)]);
```

```
Subgroup( G, [ (1,4)(2,5)(3,6) ] )
gap> IsSemiDirectProduct(g,n,k);
true
gap>
```

Function 6.2.35 The function `U(m,k)` returns the set U_m which was mentioned in Chapter 3.

```
#-------------------------------------------------------------
U := function(m,k)
local s,sigma,l,c,fs,x,i;

sigma:=RegularPerm(m,k);
l:=CoprimeList(m);
RemoveSet(l,1);
s:=[()];
for i in l do
    c:=();
    fs:=1;
    for x in CyclesOfPerm(sigma) do
      c:=c*ConjugatesTwoCycles(x,x^i,fs);
      fs:=fs+m;
    od;
    AddSet(s,c);
od;
return s;
end;
#-------------------------------------------------------------
```

Example 6.2.36

```
gap> U(5,2);
[ (), ( 2, 3, 5, 4)( 7, 8,10, 9), ( 2, 4, 5, 3)( 7, 9,10, 8),
( 2, 5)( 3, 4)( 7,10)( 8, 9) ]
gap>
```

6.3 Programs

Program 6.3.1 The permutations which conjugate $\sigma = (1, 2, \ldots, m)$ into all coprime powers of σ and fix m are sometimes all even. The following program finds such m where $2 \leqslant m \leqslant 100$.

```
#-------------------------------------------------------------
for m in [2..100] do
cpm:=CoprimeList(m);
lcpm:=Length(cpm);
foundodd:=false;
i:=1;
c:=cycle(m);
  repeat
    power:=cpm[i];
    if SignPerm(ConjugatesTwoCycles(c,c^power,m))=-1 then
     foundodd:=true;
    fi;
    i:=i+1;
  until foundodd=true or i>lcpm;
 if foundodd=false then Print(m," "); fi;
od;
Print("\n");
#-------------------------------------------------------------
```

Output:

```
2 6 9 10 14 18 22 25 26 30 34 38 42 46 49 50 54 58 62 66 70 74
78 81 82 86 90 94 98
```

Program 6.3.2 In this program first we calculate α, β and γ which generate

$G = C_m \wr S_k$. Then the direct factors of G will be printed out. By changing the values of m and k one can find out if $C_m \wr S_k$ is a direct product. Since this program first finds all the normal subgroups of G it takes a long time. Therefore it is not useful for large groups.

```
#-------------------------------------------------------------------
m:=3; k:=2;
alpha:=cycle(m); beta:=();
for i in [1..m] do
  beta:=beta*(i,m+i);
od;
if k=1 then beta:=(); fi;
gamma:=();
for i in [1..m] do
c:=();
  for j in [1..k-1] do
  c:=c*(i,j*m+i);
  od;
 gamma:=gamma*c;
od;

g:=Group(alpha,beta,gamma); g.name:="g";
Print("Finding all normal subgroups....\n");
nslist := NormalSubgroups(g);
Print("Done.\n");
nslist :=Deleted(nslist,Subgroup(g,[]));
nslist :=Deleted(nslist,g);

sizeg:=Size(g);
```

```
Print("Size of given group : ",sizeg,"\n");
sl := List(nslist,Size);
Print("Size list of proper normal subgroups of given group :\n");
Print(sl,"\n");
ln := Length(nslist);
directproduct:= false;

for i in [1..ln-1] do
  for j in [i+1..ln] do
     h:=nslist[i];
     k:=nslist[j];
     if IsInternalDirectProduct(g,h,k) then
        directproduct := true;
        Print("Given group is direct product of the ");
        Print(i,". and ",j,". \n");
        Print("subgroups in the list ");
        Print("of orders ",sl[i]," and ",sl[j],"\n");
        Print(nslist[i],"\n",nslist[j],"\n\n");
     fi;
  od;
od;

if not directproduct then
   Print("Given group is not a direct product.\n");
fi;
#-------------------------------------------------------------
```

Output:

```
Finding all normal subgroups....
```

```
Done.
Size of given group :  18
Size list of proper normal subgroups of given group :
[ 3, 3, 6, 9 ]
Given group is direct product of the 1.  and 3.
subgroups in the list of orders 3 and 6
Subgroup( g, [ (1,2,3)(4,5,6) ] )
Subgroup( g, [ (1,2,3)(4,6,5), (1,4)(2,5)(3,6) ] )
```

Output: (when m=3, k=3)

```
Finding all normal subgroups....
Done.
Size of given group :  162
Size list of proper normal subgroups of given group :
[ 3, 9, 27, 27, 54, 81 ]
Given group is not a direct product.
```

Program 6.3.3 In this program we first we calculate α, β and γ and the set U_m which generate the normaliser of a regular permutation which is a product of k disjoint m-cycles in S_{mk}. Then the direct factors of the normaliser are printed out. By changing the values of m and k one can find out if the normaliser is a direct product.

```
#-------------------------------------------------------------
m:=3; k:=2;

sigma := RegularPerm(m,k);
alpha:=cycle(m); beta:=();
for i in [1..m] do
  beta:=beta*(i,m+i);
```

```
od;
if k=1 then beta:=(); fi;

gamma:=();
for i in [1..m] do
c:=();
  for j in [1..k-1] do
  c:=c*(i,j*m+i);
  od;
 gamma:=gamma*c;
od;

Print("m=",m,",k=",k,"\n");
Print("sigma=",sigma,"\n\n");

n:=Group(Union([alpha,beta,gamma],U(m,k)),());
Print("Finding all normal subgroups....\n");
nslist := NormalSubgroups(n);
Print("Done.\n");
nslist :=Deleted(nslist,Subgroup(n,[]));
nslist :=Deleted(nslist,n);

Print("N=Normalizer of <sigma> :\n",n,"\n\n");
n.name:="N";
Print("Size of N:",Size(n),"\n\n");
sl := List(nslist,Size);
Print("Size list of proper normal subgroups is: \n",sl,"\n");
ln := Length(nslist);
directproduct:= false;
```

```
for i in [1..ln-1] do
    for j in [i+1..ln] do
        h1:=nslist[i];
        h2:=nslist[j];
        if IsInternalDirectProduct(n,h1,h2)=true then
           directproduct := true;
           Print("\nN is direct product of the ");
           Print(i,". and ",j,".\nsubgroups in the list ");
           Print("of orders ",sl[i]," and ",sl[j],"\n");
           Print(nslist[i],"\n",nslist[j],"\n\n");
         fi;
    od;
od;

if not directproduct then
   Print("\nN is not a direct product.\n\n");
fi;
#-------------------------------------------------------------
```

Output:

```
m=3,k=2
sigma=(1,2,3)(4,5,6)

Finding all normal subgroups....
Done.
N=Normalizer of <sigma> :
Group( (2,3)(5,6), (1,2,3), (1,4)(2,5)(3,6) )
```

```
Size of N:36

Size list of proper normal subgroups is:
[ 3, 3, 6, 6, 9, 18, 18, 18 ]

N is direct product of the 3.  and 4.
subgroups in the list of orders 6 and 6
Subgroup( N, [ (1,2,3)(4,5,6), (1,4)(2,6)(3,5) ] )
Subgroup( N, [ (1,2,3)(4,6,5), (1,4)(2,5)(3,6) ] )
```

Output: (when m=6, k=3)

```
m=6,k=3
sigma=( 1, 2, 3, 4, 5, 6)( 7, 8, 9,10,11,12)(13,14,15,16,17,18)

Finding all normal subgroups....
Done.
N=Normalizer of <sigma> :
Group( ( 2, 6)( 3, 5)( 8,12)( 9,11)(14,18)(15,17),
(1,2,3,4,5,6), ( 1, 7)( 2, 8)( 3, 9)( 4,10)( 5,11)( 6,12),
( 1, 7,13)( 2, 8,14)( 3, 9,15)( 4,10,16)( 5,11,17)( 6,12,18) )

Size of N:2592

Size list of proper normal subgroups is:
[ 2, 3, 4, 6, 8, 9, 12, 18, 24, 27, 36, 54, 54, 54, 72, 108,
108, 108, 216, 216, 216, 216, 216, 216, 324, 432, 432, 648,
648, 648, 648, 648, 648, 1296, 1296, 1296, 1296, 1296,
1296, 1296 ]
```

```
N is direct product of the 1.  and 35.
subgroups in the list of orders 2 and 1296
Subgroup( N,
[ ( 1, 4)( 2, 5)( 3, 6)( 7,10)( 8,11)( 9,12)(13,16)(14,17)
(15,18) ] )
Subgroup( N, [ ( 1, 5, 3)( 2, 6, 4)( 7,11, 9)( 8,12,10)
(13,17,15)(14,18,16),
( 1, 7,18, 5,11,16, 3, 9,14)( 2, 8,13, 6,12,17, 4,10,15),
( 1,16, 8, 5,14,12, 3,18,10)( 2,17, 9, 6,15, 7, 4,13,11),
( 1, 2, 3, 4, 5, 6)( 7,16,12,15,11,14,10,13, 9,18, 8,17),
( 1, 4)( 2, 3)( 5, 6)( 7,14,12,15,11,16,10,17, 9,18, 8,13) ] )


N is direct product of the 1.  and 37.
subgroups in the list of orders 2 and 1296
Subgroup( N,
[ ( 1, 4)( 2, 5)( 3, 6)( 7,10)( 8,11)( 9,12)(13,16)(14,17)
(15,18) ] )
Subgroup( N, [ ( 1, 5, 3)( 2, 6, 4)( 7,11, 9)( 8,12,10)
(13,17,15)(14,18,16),
( 1, 7,18, 5,11,16, 3, 9,14)( 2, 8,13, 6,12,17, 4,10,15),
( 1,16, 8, 5,14,12, 3,18,10)( 2,17, 9, 6,15, 7, 4,13,11),
( 1, 5, 3)( 2, 6, 4)( 7,16,12,15,11,14,10,13, 9,18, 8,17),
( 1, 4)( 2, 3)( 5, 6)( 7,14,12,15,11,16,10,17, 9,18, 8,13) ] )


N is direct product of the 1.  and 39.
subgroups in the list of orders 2 and 1296
Subgroup( N,
```

```
[ ( 1, 4)( 2, 5)( 3, 6)( 7,10)( 8,11)( 9,12)(13,16)(14,17)
(15,18) ] )
Subgroup( N, [ ( 1, 5, 3)( 2, 6, 4)( 7,11, 9)( 8,12,10)
(13,17,15)(14,18,16),
( 1, 7,18, 5,11,16, 3, 9,14)( 2, 8,13, 6,12,17, 4,10,15),
( 1,16, 8, 5,14,12, 3,18,10)( 2,17, 9, 6,15, 7, 4,13,11),
( 1, 2, 3, 4, 5, 6)( 7,16,12,15,11,14,10,13, 9,18, 8,17),
( 2, 6)( 3, 5)( 7,14,12,15,11,16,10,17, 9,18, 8,13) ] )


N is direct product of the 1.  and 40.
subgroups in the list of orders 2 and 1296
Subgroup( N,
[ ( 1, 4)( 2, 5)( 3, 6)( 7,10)( 8,11)( 9,12)(13,16)(14,17)
(15,18) ] )
Subgroup( N, [ ( 1, 5, 3)( 2, 6, 4)( 7,11, 9)( 8,12,10)
(13,17,15)(14,18,16),
( 1, 7,18, 5,11,16, 3, 9,14)( 2, 8,13, 6,12,17, 4,10,15),
( 1,16, 8, 5,14,12, 3,18,10)( 2,17, 9, 6,15, 7, 4,13,11),
( 1, 5, 3)( 2, 6, 4)( 7,16,12,15,11,14,10,13, 9,18, 8,17),
( 2, 6)( 3, 5)( 7,14,12,15,11,16,10,17, 9,18, 8,13) ] )
```

Bibliography

[1] Al–Amri, I.R. (1992). *Computational Methods in Permutation Group Theory.* PhD Thesis, University of St Andrews.

[2] Bailey, R.A.; Praeger, C.E.; Rowley, C.A.; Speed, T.P. (1983). *Generalized Wreath Products of Permutation Groups.* Proc. London Math. Soc. (3), 47, no.1, pp. 69-82.

[3] Coxeter, H.S.M. (1991). *Regular Complex Polytopes* (2nd edition). Cambridge University Press.

[4] Harary, F. (1959). *On the Group of the Composition of Two Graphs.* Duke Math. J., 26, pp. 29-34.

[5] Harary, F. (1969). *Graph Theory.* Addison–Wesley Publishing Company.

[6] Hoffmann, C.M. (1982). *Group-Theoretic Algorithms and Graph Isomorphisms.* Lecture Notes in Computer Science, Vol.136, Springer–Verlag.

[7] Humphreys, J.F. (1996). *A Course in Group Theory.* Oxford University Press.

[8] Johnson, D.L. (1970). *Minimal Relations for Certain Wreath Products of Groups.* Canad. J. Math., 22, pp. 1005-1009.

[9] Johnson, D.L. (1976). *Presentations of Groups.* Cambridge University Press.

[10] Johnson, D.L. (1980). *Topics in the Theory of Group Presentations.* Cambridge University Press.

[11] Johnson, D.L. (1990). *Presentations of Groups.* Cambridge University Press.

[12] Johnson, W. and Silver, M. (1974). *A Model for Permutation Groups.* Amer. Math. Monthly, 81, pp. 503-506.

[13] Lipscomb, S.L. (1988). *The Structure of the Centralizers of a Permutation.* Semigroup Forum, Vol.3, pp. 301-312.

[14] Neubüser, J. (1995). *An Invitation to Computational Group Theory.* Groups '93 Galway / St Andrews, London Mathematical Society Lecture Note Series, Vol.212, pp. 457–475, Cambridge University Press.

[15] Neumann, P.M. (1964). *On the Structure of Standard Wreath Products of Groups.* Math. Z., 84, pp. 343-373.

[16] Rose, J.S. (1978). *A Course on Group Theory.* Cambridge University Press.

[17] Rotman, J.J. (1973). *The Theory of Groups, An Introduction.* Allyn–Bacon, Inc.

[18] Schönert, M. et al. (1995). *GAP – Groups, Algorithms, and Programming.* Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, 5th edition.

[19] Suzuki, M. (1982). *Group Theory I.* Springer–Verlag.

[20] Wells, C. (1976). *Some Applications of the Wreath Product Construction.* Amer. Math. Monthly, 83, pp. 317-338.

[21] Wielandt, H. (1964). *Finite Permutation Groups.* Academic Press.